Aleksey Valov

UNIFIED ANTI-SPAM ANALYSER SPECIALIZED TO PROTECT FROM RUSSIAN SPAM

UNIFIED ANTI-SPAM ANALYSER SPECIALIZED TO PROTECT FROM RUSSIAN SPAM

Aleksey Valov

Bachelor's Thesis

Spring 2013

Business Information Technologies

Oulu University of Applied Science

ABSTRACT

Oulu University of Applied Sciences
Business Information Technology

Author: Aleksey Valov

Title of Bachelor's thesis: Unified anti-spam analyser specialized to protect from Russian spam.

Supervisor: Matti Viitala

Term and year of completion: Spring 2013 Number of pages: 34

The objective of the research is to analyse currently used techniques for email protection from spam and to come up with new solutions that will help to reduce the amount of Russian spam as well as the pressure on servers. The research has been performed in cooperation with Koodiviidakko in Oulu.

Descriptive research was the main methodology used during the work. Statistical analysis has been used for supporting the fight against spam as well as to increase the understanding of spam problems and commercial e-mails. Furthermore, there were clarifications of current strategies and technologies used inside the company.

The result of this research and practical implementation brought in more innovative ideas and approaches for fighting spam and increasing the amount of legitimate e-mails. The approach for anti-spam does not depend on any hardware or software.

Keywords: anti-spam, SpamAssassin, black lists, white lists, e-mail marketing, spam filter, SpamCop.

CONTENTS

1 INTRODUCTION

1.1 Background

Everyone knows what Spam is. However, for the effective anti-spam measures, there is a need to define what exactly is the meaning of spam. Internet spam is one or more unsolicited messages, sent or posted as part of a larger collection of messages, all having substantially identical content (Wellcome Trust Sanger Institute, 2012).

Quite often internet providers and the owners of the network are guided by the presumption of innocence. They relate to spam almost all emails that a recipient have not requested. By doing that, business emails can be at risk of getting lost and undelivered.

This thesis has been done with the cooperation of Koodiviidakko OY. Koodiviidakko OY, also known as Liana Technologies Ltd, is a Finnish software company working hard for the digital tomorrow. They are specialising in digital marketing and communication software of which they have more than a decade of experience. The mission of the company is to provide the best possible tools and software.

The idea of this research topic has been derived from the practical training in the company Koodiviidakko OY. The company was in need of the Russian speaking specialist in order to analyse the Russian market and to optimise their software for Spam detection of Russian emails. Another factor was the amount of spam coming daily to our email boxes that caused the necessary and important emails to be lost among them. The thesis has attempted to investigate and to create universal spam-filter that will have signature rules for Russian language.

1.2 The goal of the thesis

The on-going fight against spam has existed almost since the beginning of the intranet. Anti-spam techniques are improving and letting less and less spam to come through. However, hence the implementation of new prevention techniques, spammers are

improving their strategies as well.

Spam is holding down email marketing and all the possibilities for it to become one of the leading online marketing channels. It is flooding our mailboxes and making it impossible to see what we actually are waiting for. In order to increase the amount of legitimate emails and to reduce Spam, some old practises need to be analysed, renovated and improved for bringing the most suitable process of filtering spam in the current working environment.

In addition, pointing out the difference between spam and legitimate emails such as email marketing and newsletters was another goal of this thesis. Furthermore, as there is a demand on enhancing currently available security measures against spam, finding, testing and updating a set of rules for SpamAssassin is essential as for the company as for the individual power users.

1.3 Research methodology

Descriptive research method was chosen to be the most suitable and effective for this thesis. This method targets the analysis of the statistics and existing data. The analysed data then could be used for the development.

The exact definition of Description research is:
Descriptive research is also called Statistical Research. The main goal of this type of research is to describe the data and characteristics about what is being studied. The idea behind this type of research is to study frequencies, averages, and other statistical calculations. Although this research is highly accurate, it does not gather the causes behind a situation. (Answers Corporation, 2013.)

Descriptive research is normally used prior to the development as it collects a large sets of notes for detailed studying. It requires less time and expenses rather than quantitative experiments. However, it cannot determine what causes a specific behaviour, motivation or occurrence. In other words, it cannot establish a causal research

relationship between variables (School of Hospitality & Tourism Management, 2013.)

Statistical analysis has been used for supporting the fight against spam as well as to increase the understanding of spam problems. It has also helped to see the percentage of topics that are of most interest to spammers. Those topics have been used to analyse the SpamAssassin performance during the tests.

2 SPAM

In 1936, Hormel Foods came up with the recipe. The company initiated the contest for the product name by offering $100 as the winning prize. Kenneth Daigneau won the contest by combining two words together, sp from spiced and am from ham to create the word SPAM (SPiced hAM). In 1975, Monty Python's Flying Circus created the comedy skit wherein Vikings sing, "Spam, spam, spam, spam . . ." in a restaurant that included SPAM in each menu item. Afterwards, Internet users of Multi-User Dungeons (MUDs), bulletin boards, chat rooms and Usenet message boards began using the term SPAM for annoying, repetitive and unwanted messages. (Liana Technologies, 2012a.)

According to Dictionary.com, spam is to send unsolicited electronic mail or text messages simultaneously to a number of e-mail addresses or mobile phones (Dictionary.com, 2013). However, if a long-lost brother finds and sends to your email address_and sends you a message, this could hardly be called spam, even though it is unsolicited (Webopedia, 2013).

Mainly, Spam is used for advertising. Normally, various products and services are getting advertised through mass mailing. Furthermore, Spam is used for traffic grabbing and less common for sending viruses or malware. But all of them have the same goal of reaching the most recipients with minimum costs. Moreover, quite often senders do not care about the target audience; the amount of recipients is the key thing for them. Current estimates say that somewhere between 65 percent and 80 percent of all e-mail on the Internet is spam (Gregory, P. and Simon, M. 2005, 20).

2.1 The harmfulness of spam

First of all, the harmfulness of spam is the usage of alien resources (computers, networks, work, and money), also, breaking the national law by creating inappropriate advertisements, interference with privacy, moral damage, blocking off needed emails, spreading of viruses, etcetera. Thus, considering the amount of damage by spam it can be confidentially said that spam have been merged from the problem of individuals,

companies and governmental organisations to the problem of the society as a whole.

There are three main damages caused by spam. Firstly, the traffic of inbound emails can cause the network of recipients or companies to be flooded and to have a reduction in the needed working speed. Secondly, the loss of the working hours and productivity is another damage of spam. Without spam protection users receive more like 400 email messages each day, based on the statistic that 90% of global email traffic is spam (Allspamedup, 2009). Then, each employee categorizes spam and not spam emails that takes around 10 to 20 minutes of working time a day. Thirdly, vulnerability holes in the information security. As emails are capable of handling attachments, many Word or Excel documents can be affected by viruses. Moreover, spam can be tied to the hacking attack for breaching a security system. If the attack is succeeded, the company will have a bad reflection on the brand as well as the sensitive data will be deleted, falsified or stolen.

There are some known spamming techniques, for example, paid calls, when with the product advertisement comes in the phone number, calling to that number will result in an answer from an answering machine and you will get a connection fee. Another example is the advertisement of money pyramids. In that case, you will be promised to get rich after sending small amount of money to a certain account. Information gathering is also an example of Spam in which you will be asked to complete a survey and send it. Then the information could be used for identity theft, fraud or any other falsification. Sending of Trojans is another way to get the information, containing passwords, phone numbers, etcetera) from an unsuspecting recipient. In addition to various technical solutions, the on-going analysis of the language structure, it's changes as well as the most commonly used spam words have to be considered.

Spam does not have language barriers. Although spam written in English is the most common, it comes in all languages including Chinese, Korean and other Asian languages. 50% of spam falls into the categories of adult content, health, IT, personal finance, education and training. (Securelist, 2013)

As it has been mentioned, advertising is one of the varieties of spam. However, this is not just it for spam. There are many more existing and all the time appearing combinations. Advertising of illegal and banned products, for example, counterfeits, illegally obtained classified information, dangerous medicine. Anti-advertising of competitors as well as defame of their products or services is another variety of spam emails.

Nigerian letters aim to extort money from the recipients. The most common thing for them is that it normally includes the information on how to receive a big amount of money and the sender could help in it, after the recipient will send small sum to the sender for the purpose of document organization. The account number and personal information could be used for identity theft later on. The similarities throughout the letters they are from a "Dr." somebody, for example) are obvious, but the stories they tell are a hoot (Financial & Tax Fraud Education Associates, 2013).

Phishing is another example of the vast varieties of spam and fraud. Phish or fraudulent emails may contain links to phony websites or request you to share personal or financial information by using clever and compelling language, such as an urgent need to update your information or communicate with you to ensure the security of your accounts (Wells Fargo, 2013). It is an attempt of spammers to get credit cards information and passwords for online payment systems from the recipient of the email. Those emails are usually masked to be from the administration of the bank. That states that the recipient must confirm the information about himself or his account will be blocked, however, the form on the web-site belonging to spammers must be filled. Among the data that needs confirmation, there is sensitive information that is needed for fraudsters. For the purpose of fooling the victim, the web-site is an exact copy of the real one.

Further types of spam include chain letters, propaganda, denial of service attacks, mass mailing on behalf of another person, to create negative attitude towards him/her. Sending viruses, sniffers, Trojans and key loggers also is the purpose for spam. Furthermore, one of the usages of spam is the raising in more attraction to any particular topic.

While not as efficient as "spiders" which automatically crawl the Web in search of addresses, computer experts warn that some spammers are using chain letters to collect e-mail usernames. "Chain letters are the ideal place to collect addresses. I've seen several hundred on one e-mail. The list went on for pages," said Bill Orvis, who maintains the U.S. Department of Energy's hoax advisory Web site. (Fraser, P. 2003.)

2.2 Spam in numbers

66.7% of spam as a percentage of total inbound email. The average spam size is 3-8 Kilobytes. Around 99.5% are getting blocked by standard anti-spam rules. (Trustwave, 2013.)

As for the previous year, according to SpamCop, the average spam was 6.5 messages per second. Maximum spam was 16.9 messages per second. The total number of spam messages for the previous year was 205442708. (SpamCop, 2013.)

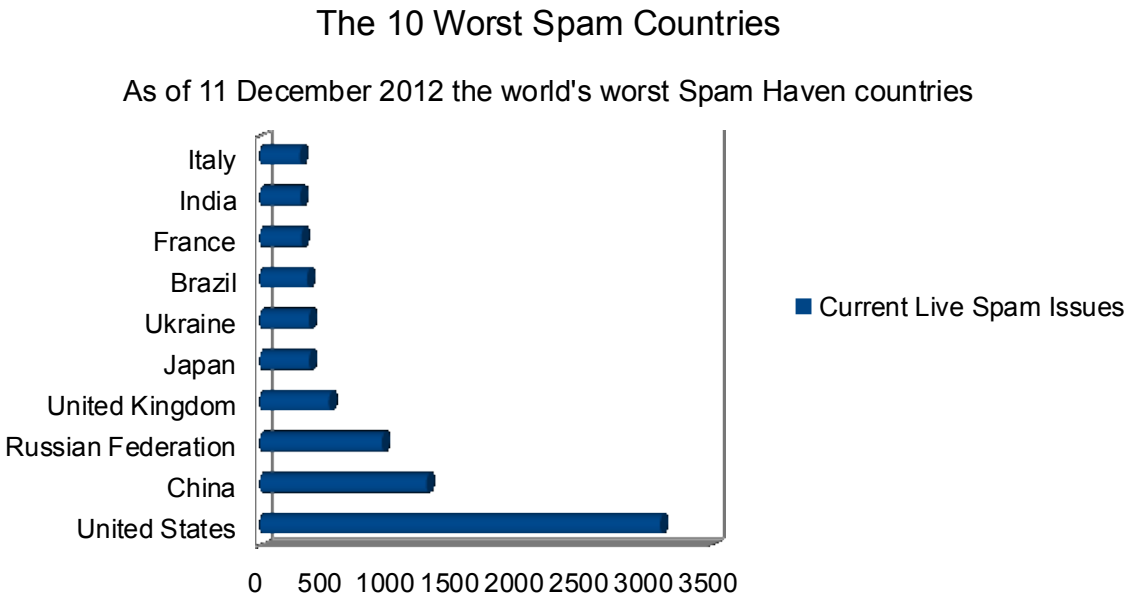

Figure 1 The 10 worst spam countries.

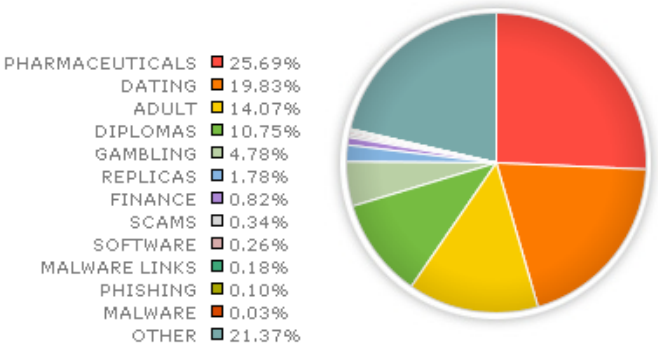

Figure 2 Spam by category (Trustwave, 2013).

As seen from the figure 1, Russia is on the 3rd place of being the worst spamming country. Hence, the amount of Russian spam is still big. Figure 2 reflects the universal spam categories.

3 EMAIL MARKETING

Email marketing is a form of direct marketing. It uses emails as a commercial communication with push marketing strategy. Email marketing compliments with other marketing techniques for distributing correct marketing message. (Liana Technologies, 2012b.)

In email marketing there are numerous ways of creating a communication channel with potential or existing clients. The difference of that from advertising is the access to mass end-consumers with personalized level. One of the first questions to do that is why. The cornerstone of the strategy of such marketing is to provoke a desire among consumers to create a dialogue with the sender of the message, to respond to the message and to establish a personal relationship with him.

Today, when the amount of offerings on the market of products and services exceeds the demand, companies that work in the same business sphere offer quite similar services and products with a slight difference in price. Under these circumstances there is a need in some additional incentives that tie the consumer to the supplier. Most companies are using common techniques for winning the loyalty of clients, for example, bonus programs, client cards, accumulated discounts. This situation are beaten track, trying to cause customer loyalty through material rewards for purchases made (bonus programs, card patrons, accumulated discounts). However, the loyalty created in such way is very fragile, and the consumer will not hesitate to switch to a competitor if he will have more discounts or other benefits.

Quite often clients use services of the company that they feel more comfortable with. Such emotional attitude can only be created through the interaction with the customer on a personal level, because it is the personal touch that is left in the minds with a bright trace. Email marketing offers to establish personalized communications with customers, access to their emotions and personal account of the needs of each client.

Each email marketing campaign starts with putting on objectives. Depending on that the

invitation to the presentation or sales, supporting of the loyalty of current customers, attracting new consumers or promotions of products will result in different ways of communication. There will be also a need to be certain if the sales and promotions are a onetime event or happen to be in an everyday communication with clients.

Think of an e-mail campaign as being an extension of your other advertising strategies. You don't want to replace them entirely, but you can add the hottest sizzle in town by using e-mail. The reason e-mail is hot is that you can target so effectively. You can be wildly creative — embedding audio and video and inter- active capabilities in your messages — for relatively little expense. (Dahl, G. 2007, 92.)

The figure below shows the whole concept over email marketing. Gathering contacts and information about potential as well as current clients in addition to the market and product or service analysis brings in the ability to personalized communication with them. Explaining those who gave the permission to receive emails about the benefits of the particular product, service or discount increases the loyalty of the recipients to that company.

Figure 3 Methods of gathering and utilizing contact information (Liana Technologies, 2012c).

4 FIGHTING SPAM

The best way for fighting spam is to not let spammers to know the email address. That is a hard task, but there are some precautions that could be made. One of the advices is not to publish the address on public sites.

If there is a need to publish an email address, it can be encoded in such way “user (@) domain.net”. Spammers use special software for scanning sites and gathering of email addresses and this kind of encoding might not help. Any simple encodings could be picked up by scanners. Furthermore, the encoding creates discomfort not just for spammers, but for regular web-site visitors as well.

Many public sites do not publish email addresses of registered users. All the messages could be sent to the nickname of another user. The real address is substituted by the server using the profile information of the user that is otherwise invisible to others.

The address could be inputted as an image. There are numerous online services for doing that automatically; however, some of them can gather inputted email address themselves. Besides online services the transformation to the image could be done with the help of any graphical editor or by handwriting the email and taking a picture of it. JavaScript could be used to encode the address on web-pages.

Another approach for fighting spam is to create any additional email address for registering at services that are doubtful and not used for daily work. Online services that create onetime emails for that purpose could be found easily. Mailinator is one of the most popular.

Mailinator is a different kind of email service. The biggest difference is that you don't need to sign up. Any email name could be registered at the service. The email existswhen you create them and they are just waiting for you to check your inbox. (ManyBrain, 2012.)

Never answering to spam or following the links inside of it reduces the amount of tracking and can mislead the spammer into thinking that the address is inactive. If not done so, the amount of spam can be increased drastically. The loading of pictures in the email can be also used for tracking the activeness of the email upon reading. Providing spammers with as less information and statistics as possible is one of the keys to reduce the amount of them.

All the previously mentioned methods for hiding the address has a principal disadvantage of creating inconvenience for the ones who need to read the address. Furthermore, quite often the address has to be published for example for the information on the company. Moreover, hiding contact information could be treated dangerously by search engines.

Automatic filtering is achieved through special software for automatic spam detection. This software could be installed on the server or client side. It normally has two main approaches.

The first one analyses the content of the received email and draws conclusions whether it is spam or not. The email thought to be spam is separated from the rest of emails or it could be marked and inputted in a special folder. That type of software could work on the server or client side. In the method for the client, he or she does not see the email, but the drawbacks associated with its administration still exist as the software firstly receives the mail and then filters it. The software on the server side does not reflect on computer resources of the client, but can result in mistakes in spam recognition that will create a risk of not receiving the intended business email.

The second approach uses various methods for marking the sender as a spammer without looking into the content of the email. That type of software could only work on a server handling incoming emails. In such way, additional traffic is used by the server for communicating with email systems of spammers and requests to other servers for checking.

White lists, also known as Safe Lists, are one of the most popular technologies that work together with self-taught filters, systems with pattern searches and systems that query senders. White lists include only people who proved themselves as reliable and proper senders. Usually those people are individuals, even-though, some systems could have also domain names. In case of being white listed, if the intellectual spam filter marks the email as spam, it will still be delivered to the intended recipient. This method of blocking the spam reduces the amount of false positives. White lists require constant maintenance to be very effective, if not properly maintained, the risk of losing e-mail from legitimate sources is high (Postcastserver, 2013).

Some email administrators preferring whitelists in a different manner. By doing so, they let in only the emails of senders from that whitelist and the rest will go to spam. The recipient can check the spam folder from time to time and choose emails that should not be there. This approach is most suitable for people who do not receive much emails or whose communication is predefined and known. As business wise that does not work well as one of the key elements of any business is to get new clients.

All in all, white lists are not reliable enough. Due to the protocol used, spoofing the address of the sender is very simple and anyone could use a different name. That's why we could receive emails from ourselves as many users add themselves or friends to the whitelist.

Black list is a list of IP addresses and domains of known spam e-mail servers and are used to block all e-mail that comes from certain servers on the Internet that have been identified as being used to send spam (Postcastserver, 2013). There is a need to choose a reliable provider with an integrated spam filter. Most providers are working with official databases that have the information on domain names, IP and email addresses that have been used to send spam. Providers block the addresses from those databases. One of the most widely used services with the database of spam addresses is Spamhause. Spamhaus tracks the Internet's spam senders and spam services, provides dependable real-time anti-spam protection for Internet networks, and works with Law

Enforcement to identify and pursue spammers worldwide (Spamhause, 2013). If provider does not filter spam or does it incorrectly or if the email needs to be used, but is under attack of spammers, it is advised to install the security layer from spam by using databases of Spamhause.

Most of the email providers have the feature of Black lists or Anti-spam. However, new spammers appear on a daily basis, in order to fight them requires the maintenance as well as upgrading of databases. If anti-spam filters have not blocked an email that is more likely spam, administrators should be notified and take an action. Spamhause is maintaining databases, considers questions about the deletion of addresses from databases, but does not act on the complaints on spam and mass mailings.

According to Evan Harris, grey lists got its name because it is kind of a cross between black- and white-listing, with mostly automatic maintenance (Harris, 2004). It only looks at three pieces of information such as IP address, sender's address and recipient's address. The method of greylisting relies on the special behaviour of spammer's software that will not try to resend the letter if there is a temporary problem as requested by SMTP protocol. In addition, spammers are using false names and return addresses in order to get around security of a system, that’s why the receiver thinks that it receives various emails from various senders.

The simplest executing process of grey lists goes as the following: all SMTP servers that have not been known go to grey checking. All the emails from those servers neither are processed nor put in spam; the receiving server is sending the temporary error request to the sender. In case if the sender tries to resend the email after some time, the email will go to a white list, otherwise it will be black listed. That is reason sometimes to get emails later then they supposed to come. Around 90% of spam is getting filtered without any risk for legitimate emails (Harris, 2004).

However, that method is not perfect. Some emails that do not follow SMTP protocol could be put aside, for example, newsletters from news websites. Servers with such behaviour should be put in white lists, if possible.

The delay between deliveries could increase up to half an hour that is unacceptable for urgent cases. That disadvantage is compensated in a way that only first deliveries from unknown recipient are delayed. Furthermore, most grey lists approaches automatically add known senders to the white list. There is a possibility to have server sharing of those lists that will result in a delay of less than 20% of emails.

Some companies use several delivery servers with different IP addresses. In that case, the same email could be sent from two or more different IP addresses. That could result in a delay. Normally the ranges of trusted senders are added to white lists.

The software of spammers is continuously improved. The support of the resending of emails could be easily implemented, making that defence approach irrelevant. The key aspect of that defence method is the time ratio of spammers to get into the black lists to the time of the delay of grey lists. Grey lists are useless in a long term, but create an additional barrier for spammers.

Other methods such as the restriction of requirements for emails and senders, for example, denial of processing email with incorrect return address or non-existent domain, double checking of the domain name and IP address of the sender, etcetera, are simple to implement. The mentioned approaches get rid of just simple spam. However, they still get some, thus, worse of implementing.

Sorting email depending on the topic is another good idea to categorize spam. Some email clients, such as Mozilla Thunderbird, provide the opportunity to analyse just the topic of an email. That reduces the network traffic as the client could download the full message only if the topic was right for him or her.

The type of systems “call-answer” makes sure that the sender is a human being rather than automated software. That approach demands from the sender additional actions that are not often welcomed. Most those system's types create additional load on email systems. Furthermore, that system cannot clearly distinguish between automated

spamming software and newsletter software.

There are other systems determining the mass of emails, such as Razor or Distributed Checksum Clearinghouse. Software integrated into the email server modules count the checksum for each incoming email and check them on servers of Razor and DCC that report the amount of showing of that email on the web. On the other side, mass emails could come from legitimate newsletters. Moreover, spammers can have various content, for example, adding random characters to the end of the letter.

There is a clear view of overall changing in the ideology of emails processing. In order to receive the email by the server, each sender's system should perform additional phases that sometimes could be quite demanding, for example, various mathematical algorithms. As for the average email sender there will be no problem to do so, however, spammers will get more barriers and problems for sending millions or even billions of emails.

5 SPAMASSASSIN

SpamAssassin is a mature, widely-deployed open source project that serves as a mail filter to identify Spam. SpamAssassin uses a variety of mechanisms including header and text analysis, Bayesian filtering, DNS block lists, and collaborative filtering databases. SpamAssassin runs on a server, and filters spam before it reaches your mailbox. (SpamAssassin, 2012.)

SpamAssassin is written on Perl programming language, thus, it relies on Perl modules. Those Perl modules together with SpamAssassin could be installed through Comprehensive Perl Archive Network, a large collection of Perl software and documentation, also known as cpan (CPAN, 2013). SpamAssassin could be found in cpan as a module with a name Mail::SpamAssassin. As cpan comes with every perl installation, it is installed almost on every server.

SpamAssassin is an Apache Foundation project. Apache is known for its web server solutions. Furthermore, SpamAssassin is absolutely free as it is open source. The filter's community is also vast.

SpamAssassin is used for filtering incoming emails for one or several recipients. It can be run as a standalone application or as a subprogram of another application (such as Milter, SA-Exim, Exiscan, MailScanner, MIMEDefang, Amavis) or as a client, spamc, that communicates with a daemon, spamd (Zaped, 2013). The last process is the most efficient, however, could cause a danger to the security system.

SpamAssassin comes with a wide selection of rules that determine which emails is spam. Most of those rules rely on regular expressions that belong to the body or header of the email. In addition, SpamAssassin uses various techniques for spam identification. All of them are in the documentation in SpamAssassin under “tests”.

Every single test has points. If an email passes the test, those points are added to the

overall amount of points. Points could be either positive or negative. Positive amount is spam, but negative – ham. The email goes through all tests with the overall calculated amount of points. The higher points give the higher chance of an email to be marked spam.

SpamAssassin has the adjustable amount of points for an email to be considered as spam. Usually that level is set in such way that triggering just one rule will not result in a spam mark. However, there are cases when two or more triggered rules give as a result false positives.

SpamAssassin relies on Bayesian filtering. Bayesian spam filter checks a message its probability to be spam. Unlike simple content-based filters, Bayesian spam filtering learns from spam and from good mail, resulting in a very robust, adapting and efficient anti-spam approach that, best of all, returns hardly any false positives (Tschabitscher. 2013). Bayesian filter looks into the words, headers, HTML code, word pairs, phrases and meta information.

The Bayesian method is not language dependent, thus the anti-spam filter could be used with any required language. However, most keywords, triggers and rules were meant to be for the English language only. These intellectual abilities make it possible to filter and catch more spam.

The real advantage of the Bayesian approach is that you know what you're measuring. The Bayesian approach assigns an actual probability. The problem with a "score" is that no one knows what it means. (Graham, P. 2004, 113.)

6 SPAMCOP

SpamCop is the premier service for reporting spam. It has three main duties as explained on the website of SpamCop. Report spam to help Internet providers cut spam off at the source. Professional-grade SpamCop email accounts feature spam reporting, customizable spam and virus filtering and simultaneous Webmail, POP and IMAP access. SpamCop DNS-based Blocking Lists can be used with any mailserver to get safe and effective spam filtering for free. (SpamCop, 2012.)

If an email user receives much spam and do not know how to block it, he will have a possibility to do so through SpamCop. SpamCop determines the origin of unwanted emails and then sends complain to the service provider. Those service providers supposed to block spammers that use their services.

In order to report spam through SpamCop, there is a need to register an account on their website. Afterwards, the confirmation email will be send and the login details will be provided. Then, the full email, containing headers as well, should be inputted into the special form.

Headers contain tracking information for an individual email, detailing the path a message took as it crossed mail servers (Google, 2013). For example, in Gmail after clicking Reply, there is a possibility to Show Original that will include all the headers. In Apple Mail, headers are visible after clicking View-Message-All Headers.

That approach of reporting spam does not guaranty the instant blocking of spammers, however, the information about the abuse will be forwarded to his service provider that will take care of him. Furthermore, those reports are considered during database updates for various spam filters. It is one of the ways how the IP addresses of spammers get into the official databases of spam sources that are used by numerous email providers.

7 INSTALLATION AND IMPLEMENTATION OF THE ANTI-SPAM SOLUTION

In the beginning of the practical execution, there was a need to choose the filter to work with. That choice fell onto SpamAssassin and its testing on the fresh installation of Mac OS X. SpamAssassin is the ultimate spam filter that could be found as a non-commercial project. Furthermore, SpamAssassin is widely adapted by email providers and some power computer users. In addition, that particular spam filter was used inside Liana Technologies Ltd.

After the analysis of possibilities to change and the flexibility of SpamAssassin I had to find the information on how to integrate SpamAssassin on Mac OS X. There was a lot of materials available on how to do the whole installation. However, not all of them were as complex as needed; for example, the official SpamAssassin guide did not cover all the additional perl modules required for better performance and full installation. In addition, there was no information on that guide how to install Developer Tools on Mac OS X.

As I already had an Apple ID, it was much easier to register as an Apple developer. Registering for free as an Apple developer gives the access to Apple developer tools and resources for creating iOS and Mac apps, including Xcode, WWDC videos, sample code, and more (Apple, 2012). After that, I was able to install Xcode from the Mac App Store. Xcode is a package provided by Apple containing compilers, libraries and additional tools required to develop applications for Mac OS X (Macports, 2012).

Once the installation is done, Xcode should be opened for the installation of Command Line Tools as shown on the figure below. That option is available at Xcode > Preferences > Downloads and you will see the option to install the “Command Line Tools” (Andrademilton, 2012).

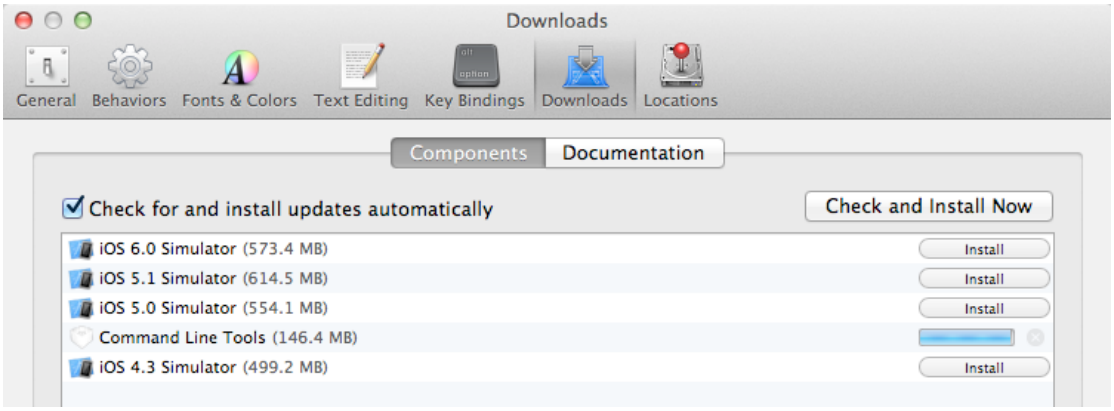

Figure 4 Installing Command Line Tools on Xcode.

The next phase was the installation of various Perl modules. As been a perl developer, I installed YAML module at first. YAML is a human friendly data serialization standard for all programming languages (Evans, 2011). Furthermore, YAML is much better for developing, managing, reading and writing configuration files. Afterwards, I moved to the installation of SpamAssassin and other Perl modules. The following figure shows the process of installation in Terminal.

```
Documents — bash — 82×24
Alekseys-MacBook-Pro:Documents Xenos$ sudo cpan -i Mail::SpamAssassin Net::DNS Dig
est::MD5 Digest::HMAC MIME::Base64 Mail::Internet MIME::Entity Time::HiRes Mail::A
udit Mail::POP3Client
CPAN: Storable loaded ok (v2.22)
Reading '/Users/Xenos/.cpan/Metadata'
  Database was generated on Tue, 26 Mar 2013 15:17:02 GMT
CPAN: Module::CoreList loaded ok (v2.43)
Mail::SpamAssassin is up to date (3.003002).
Net::DNS is up to date (0.72).
Running install for module 'Digest::MD5'
Running make for G/GA/GAAS/Digest-MD5-2.52.tar.gz
CPAN: LWP::UserAgent loaded ok (v5.835)
CPAN: Time::HiRes loaded ok (v1.9719)
Fetching with LWP:
ftp://ftp.osuosl.org/pub/CPAN/authors/id/G/GA/GAAS/Digest-MD5-2.52.tar.gz
CPAN: YAML loaded ok (v0.84)
CPAN: Digest::SHA loaded ok (v5.47)
Fetching with LWP:
ftp://ftp.osuosl.org/pub/CPAN/authors/id/G/GA/GAAS/CHECKSUMS
CPAN: Compress::Zlib loaded ok (v2.024)
Checksum for /Users/Xenos/.cpan/sources/authors/id/G/GA/GAAS/Digest-MD5-2.52.tar.g
z ok
CPAN: Archive::Tar loaded ok (v1.54)
CPAN: File::Temp loaded ok (v0.22)
```

Figure 5 Installing SpamAssassin and various Perl modules from CPAN.

I used sa-update utility that comes with SpamAssassin's installation to get new rules from the official repository of SpamAssassin. sa-update automates the process of downloading and installing new rules and configuration, based on channels (Manpagez, 2013). However, there was an error during the execution of the update that was resolved by adding the flag nogpg.

Razor extensions could be installed in addition to SpamAssassin. Razor is a distributed, collaborative, spam detection and filtering network (Prakash, 2013). Furthermore, DCC could be also installed. The Distributed Checksum Clearinghouses or DCC is an anti-spam content filter that runs on a variety of operating systems (Rhyolite, 2013). However, those two extensions were out of scope of this thesis as the goal was targeting mainly the rules for SpamAssassin.

7.1 Russian rules for SpamAssassin

SpamAssassin checks every incoming email against it's rules. Any word, combination of words or a sentence could trigger it and give a certain amount of points that will result in a decision whether to mark the email as spam or not. Therefore, sometimes the generic rules are not enough to catch all annoying spam. Anti-spam tests and configuration are stored in plain text, making it easy to configure and add new rules (SpamAssassin, 2013).

In the beginning of creating my rules for the filter I searched the internet in order to find how to add, create and configure new rules. Furthermore, I found the already made set of Russian rules with various encodings.

Russian ruleset for SpamAssassin filtering engine. Place the file 99_russian_re.cf to the directory where all other ruleset files reside (usually /usr/share/spamassassin) and restart spamd by SIGHUP. The set of keywords, used for building the rules file is found in the file tokens.utf-8. (Sa-russian, 2013.)

After downloading that set of russian rules for SpamAssassin, there was a choice of rules for various cyrillic encodings. Koi8-r was the encoding of the choice as it was preferred for the commissioner. Afterwards, I made sure to put the rules in the right place of my installation. As it was mentioned by Darxus not to put any .cf rules under /usr/share/spamassassin, the rules were added to /etc/mail/spamassassin (Darxus, 2011).

7.2 Testing and results

After the installation of SpamAssassin and rules configuration, the time came for testing. First of all, the rules were tested by SpamAssassin on the correctness of the syntax. For that purpose I used the flag of SpamAssassin called lint. However, just lint was not enough. D is an additional flag to lint for debugging purposes that was used. The testing showed no errors for the added rules.

The second testing included the real detection of emails from my old personal email box that contained a lot of spam. For that purpose a separate installation of Mozilla Thunderbird was made. Then SpamAssassin filtering was checked on to be the junk filter for the account with personal emails as shown on the figure below.

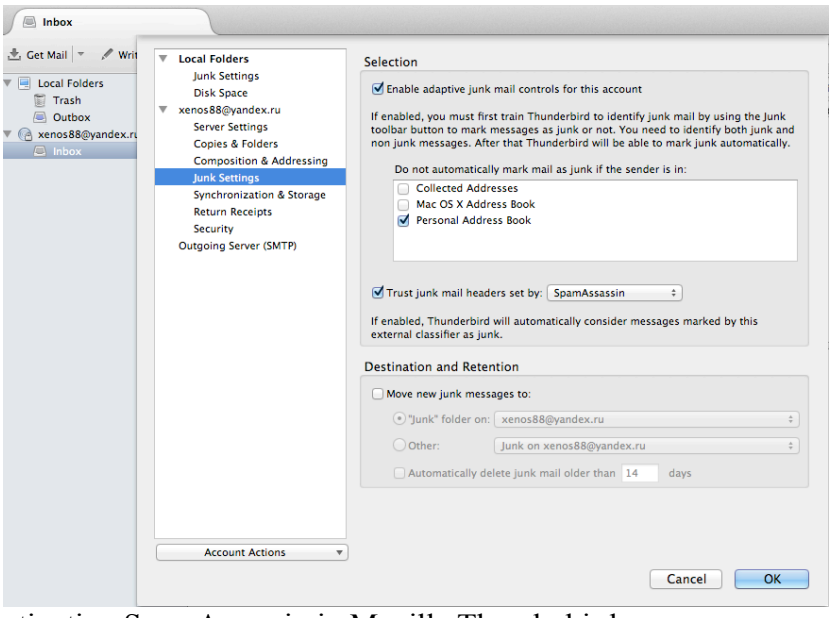

Figure 6 Activating SpamAssassin in Mozilla Thunderbird.

SpamAssassin did filter spam, however, most of it was in english language. Only

several spam emails were caught in russian language. Those emails contained mostly erotic content that made it easy for SpamAssassin to catch it. However, there were some false positives. The figure below shows some of the messages that got into spam.

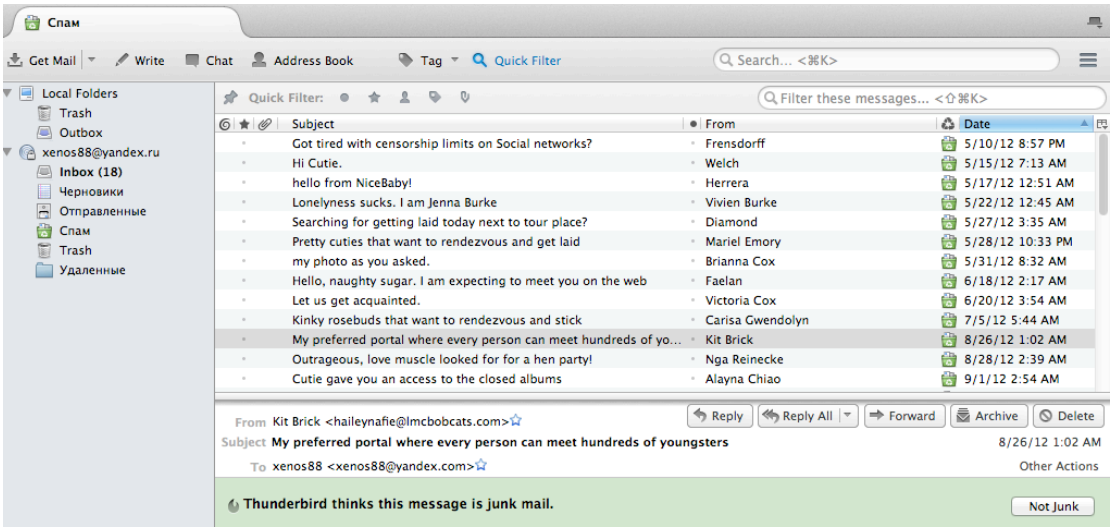

Figure 7 Spam filtering in Mozilla Thunderbird.

Such behaviour of SpamAssassin as well as the small percentage of spam was a result of Yandex filtering spam as well. In addition, SpamAssassin together with Mozilla Thunderbird needed training in order to have the increase of chances to catch spam and to have less false positives.

The performed test did not check all the aspects of spam rules. That is why there was another test. The other part of testing was three months of checking my personal emails by SpamAssassin. During that time, the spam filter was taught of legitimate emails as well as of spam. However, the spam folder needed to be checked once in a while as there was a chance to have wrongly marked legitimate emails. By putting those emails back to the inbox folder or adding the sender's address to a self-managed white list, improved the correctness of SpamAssassin over a week or two.

8 CONCLUSION

All in all, goals of the thesis were met to a certain extent as there was time and other factors involved. The testing process took most of the time without requiring much of any other resources. Furthermore, the whole process was a matter of mistakes and finding the ways to overcome them. Some spam emails that were added to the system could cause mostly all the emails to be in spam, even if they were from legitimate sources.

Spam is undoubtedly the result of uncontrolled and unpredictable emergence of the global network. Effective approaches on fighting spam are known, however, there are still new spammers appearing every day as the entrance barrier is very low. Moreover, the companies think that by using mass mailing and sending advertisements of their brilliant products and services will result in a huge revenue and attraction. Obviously, there will be attraction, but of a bit different than expected as nobody likes to receive spam. In case of making spam economically viable, the problem might disappear at all.

8.1 Limitations and implications for the future research

The spam filter teaching almost never ends, because spammers create something new all the time. In addition, the spam trends do change over time, for example, the mortgage topic was of an interest for spammers before the financial crisis in 2007-2008. Now mortgage topics are not risen very often.

Besides the teaching and adapting the spam filter towards any particular needs, the analysis of words, word combinations and sentences should be considered. The deep knowledge of the language can help in developing the rules further. Moreover, the number of rules for SpamAssassin, that is considered the best and most widely accepted solution, could be indefinite. However, it should not be forgotten that the higher verification level could result in a higher chances of false positives.

REFERENCES

Allspamedup, 2009, Is spam prevention too costly for your business? Date of retrieval 17.02.2013 http://www.allspammedup.com/2009/02/is-spam-prevention-too-costly-for-your-business/

Andrademilton, 2012. How to install Xcode 4.3.2 with Command Line Tools – Mac OS X. Date of retrieval 15.09.2012 http://andrademilton.com/2012/04/29/how-to-install-xcode-4-3-2-with-command-line-tools-mac-os-x/

Answers Corporation, 2013. What is descriptive research? Date of retrieval 13.02.2013 http://wiki.answers.com/Q/What_is_descriptive_research

Apple, 2012. Register as an Apple Developer. Date of retrieval 15.09.2012 https://developer.apple.com/programs/register/

CPAN, 2013. CPAN Frequently Asked Questions. Date of retrieval 23.03.2013 http://www.cpan.org/misc/cpan-faq.html#What_is_CPAN

Dahl, G. (2007). Advertising for Dummies. New Jersey: Wiley Publishing, Inc.

Darxus, 2011. WritingRules. Date of retrieval 20.09.2012 http://wiki.apache.org/spamassassin/WritingRules

Dictionary.com, 2013. Spam. Date of retrieval 17.02.2013 http://dictionary.reference.com/browse/spam

Evans, C., 2011. YAML. Date of retrieval 16.09.2012 http://yaml.org/

Financial & Tax Fraud Education Associates, 2013. Nigerian Scam Letter Exhibit. Date of retrieval 23.02.2013

http://www.quatloos.com/cm-niger/nigerian_scam_letter_museum.htm

Fraser, P. 2003. How some spammers get your e-mail. CNN 02 September 2003.

Google, 2013. Message headers. Date of retrieval 24.03.2013
http://support.google.com/mail/answer/22454?hl=en

Graham, P. (2004). Hackers and Painters: Big Ideas from the Computer Age. USA: O'Reilly Media, Inc.

Gregory, P. and Simon, M. (2005). Blocking Spam & Spyware for Dummies. New Jersey: Wiley Publishing, Inc.
http://www.lianamailer.com/capabilities.html

Harris, E., 2004. The Next Step in the Spam Control War: Greylisting. Date of retrieval 15.03.2013
http://projects.puremagic.com/greylisting/whitepaper.html

Liana Technologies, 2012a. Anti-Spam Policy. Date of retrieval 17.02.2013
http://www.lianamailer.com/resources/anti-spam.html

Liana Technologies, 2012b. Capabilities. Date of retrieval 23.02.2013
http://www.lianamailer.com/capabilities.html

Liana Technologies, 2012c. What is email marketing. Date of retrieval 23.02.2013
http://www.lianamailer.com/resources/tutorials/what-is-e-mail-marketing.html

Macports, 2012. Install Xcode. Date of retrieval 15.09.2012
http://guide.macports.org/chunked/installing.xcode.html

Manpagez, 2013. Sa-update. Date of retrieval 16.09.2012
http://www.manpagez.com/man/1/sa-update/

ManyBrain, 2013. Mailinator FAQs. Date of retrieval 24.02.2013
http://www.mailinator.com/faq.jsp

Postcastserver, 2013. Internet Black and White Lists. Date of retrieval 11.03.2013
http://www.postcastserver.com/help/Internet_Black_and_White_Lists.aspx

Prakash, 2013. Vipul's Razor. Date of retrieval 26.03.2013 http://razor.sourceforge.net/

Rhyolite, 2013. Distributed Checksum Clearinghouses. Date of retrieval 26.03.2013
http://www.rhyolite.com/dcc/

Sa-russian, 2013. Russian ruleset for SpamAssassin. Date of retrieval 26.03.2013
http://sa-russian.narod.ru/

School of Hospitality & Tourism Management, 2013. Descriptive research. Date of retrieval 13.02.2013
http://www.htm.uoguelph.ca/MJResearch/ResearchProcess/DescriptiveResearch.htm

Securelist, 2013. Types of spam. Date of retrieval 23.02.2013
http://www.securelist.com/en/threats/spam?chapter=88

SpamAssassin, 2012. Welcome to SpamAssassin. Date of retrieval 17.03.2013
http://wiki.apache.org/spamassassin/

SpamAssassin, 2013. The Apache SpamAssassin Project. Date of retrieval 26.03.2013
http://spamassassin.apache.org/

SpamCop, 2012. SpamCop. Date of retrieval 24.03.2013 http://www.spamcop.net/

SpamCop, 2013. SpamCop Statistics. Date of retrieval 23.02.2013
http://www.spamcop.net/spamgraph.shtml?spamyear

Spamhaus, 2012. The 10 Worst Spam Countries. Date of retrieval 11.12.2012
http://www.spamhaus.org/statistics/countries/

Spamhaus, 2013. The Spamhaus project. Date of retrieval 11.03.2013
http://www.spamhaus.org/

Trustwave, 2013. Spam Statistics. Date of retrieval 23.02.2013
https://www.trustwave.com/support/labs/spam_statistics.asp

Tschabitscher, H, 2013.What You Need to Know About Bayesian Spam Filtering. Date of retrieval 23.03.2013
http://email.about.com/cs/bayesianfilters/a/bayesian_filter_2.htm

Webopedia, 2013. Spam. Date of retrieval 17.02.2013
http://www.webopedia.com/TERM/S/spam.html

Wellcome Trust Sanger Institute, 2012. Wellcome Trust Sanger Institute Anti-Spam Policy. Date of retrieval 05.11.2012 http://www.sanger.ac.uk/legal/spam.html

Wells Fargo, 2013. Report Phish and Email Scams. Date of retrieval 23.02.2013
https://www.wellsfargo.com/privacy_security/fraud/report/fraud

Zapped, 2013. SpamAssassin. Date of retrieval 23.03.2013
http://www.zaped.info/Spam_Assassin