TOWARDS SECURITY AND BALANCE IN EMAIL THROUGH CORRESPONDENCE NEGOTIATION

by

Muhammad Mahmood Riyadh
B. Sc, University of Windsor, 2001

A PROJECT SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

In the
School of Computing Science

SIMON FRASER UNIVERSITY

Summer 2005

APPROVAL

Name: **Muhammad Mahmood Riyadh**

Degree: **Master of Science**

Title of Project: **TOWARDS SECURITY AND BALANCE IN EMAIL THROUGH CORRESPONDENCE NEGOTIATION**

Examining Committee:

Dr. Jiangchuan Liu
Assistant Professor, School of Computing Science
Chair

____

Dr. Robert D. Cameron
Professor, School of Computing Science
Senior Supervisor

____

Dr. Fred Popowich
Professor, School of Computing Science
Supervisor

____

Dr. Richard K. Smith
Associate Professor, School of Communication
Examiner

Date Defended/Approved: July 20, 2005

SIMON FRASER UNIVERSITY

PARTIAL COPYRIGHT LICENCE

ABSTRACT

Email has emerged as a preferred communication medium among people of all generations. With the increasing number of users, SPAM has become a major cause of concern. Spammers are taking advantage of vulnerability of the email transport and delivery protocol (SMTP), to spread viruses, send fraudulent messages, etc. Consequently, the current email system suffers from lack of security, and imbalance between senders and receivers. This work introduces Correspondence Negotiation Protocol (CNP) to make email communication more secure. We address the current imbalance between senders and receivers, and try to solve this imbalance by providing more control to recipients and making senders more accountable. We present an implementation of Correspondence Negotiation Agent (CNA) - an email client that supports CNP. CNA is composed of three principal components: Authenticator, Negotiator, and eSecretary. It has been implemented by extending JMail. CNA runs on multiple operating systems and can inter-operate with other email clients.

DEDICATION

To My Parents!

ACKNOWLEDGEMENTS

I would like to take this opportunity to make an attempt to express my gratitude towards all those people who have played an important role in some way or another to help me complete this work.

I am deeply indebted to my senior supervisor Dr. Robert D. Cameron. This work would not be in the form it is today without his intellectual inputs and advice. He has inspired my efforts through his own sincere interest in this area of email communication. His stimulating suggestions, encouragement, and support helped me in all the time of research. I have learned many things from him, and it has been a great pleasure for me to work with him.

I want to thank my supervisor Dr. Fred Popowich and examiner Dr. Richard Smith for their constructive comments on this report. I want to thank Dr. Jiangchuan Liu for coordinating my defence professionally.

I would like to thank my parents without whom I would not be in a position where I am right now. I would also like to thank my wife Taskin for her continuous support during my studies.

I must also extend my gratitude to the faculty and staff in the School of Computing Science at SFU for providing an environment conducive to world-class research.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

GLOSSARY

1. **CNP** – Correspondence Negotiation Protocol.
2. **CNA** – Correspondence Negotiation Agent.
3. **SMTP** – Simple Mail Transfer Protocol.
4. **SPAM** – Unsolicited Bulk Email.
5. **MUA** – Mail User Agent.
6. **MTA** – Mail Transport Agent.
7. **DNS** – Domain Name System.
8. **ASRG** – Anti-Spam Research Group.
9. **RFC** – Request for Comments.
10. **IETF** – The Internet Engineering Task Force.

1 INTRODUCTION

1.1 Goal

The goal of the Correspondence Negotiation Protocol (CNP) is to address socio-technical flaws in current e-mail standards and technology through a new, upwards-compatible protocol layer. The work is to make email more secure, provide a balanced communication between senders and receivers, and explore the usage of this widely used communication medium, i.e. increasing the usability of email messaging.

1.1.1 Secured and Balanced Protocol

It is not very difficult to realize why email should be made more secure. Anyone who uses email would agree as s/he has had some bad experience with it already. These could imply receiving unsolicited emails, being affected by worms/viruses through email, and being deceived by fraudulent emails (phishing), etc. This problem of unwanted email can be minimized if we can make sure that the recipient receives emails, which s/he believes important to him/her. So, CNP would try to make sure that the recipient does not have to see or spend time on an email that s/he considers spam.

1.1.2 Usage of Email

Email provides convenient, time-saving communication with family members, friends, co-workers, partners and customers. It is an essential part of business today. It has become the primary business productivity application. A study has revealed that, over 80% of workers in the US and Canada report using email daily or several times each week [30]. The same study has shown that users preferred email as much as 5 times more than face-to-face or phone calls for exchange of regular information. Since more and more people are using email as their preferred means of communication, CNP would look into ways to increase the usage of this tool, such as automatic scheduling, instant messaging, collaboration, role based communications, automatic interactions, threading messages, grouping messages, etc. It can also be used as an automatic information system (similar to an automated telephone information service).

1.2 Motivation

Simple Mail Transfer Protocol (SMTP) was developed at a time when only a few clients and servers existed. SMTP does not have sufficient security features, especially considering the broad range of internet users today [1, 28]. Originally, any SMTP server would accept mail from anyone, for anyone. This is known as open relay[1]. This wasn't a problem in the early days of the Internet, but some time ago it became a real threat. Open relay is no longer an issue for the majority of companies these days. This is because the Administrators have closed open relays. If there are any open relays they will be relatively quickly listed on open relay blocklists like Spamhaus (www.spamhaus.org), ORDB (www.ordb.org) and many more. The biggest problem today is mail that is

[1] An open mail relay occurs when a mail server processes an email message where neither the sender nor the recipient is a local user.

correctly addressed to a valid mail address, but comes from a dubious source [28]. Fraudulent e-mails (phishing) exploit a loophole in the SMTP protocol which allows ISP's mail servers (where e-mails are received) to accept messages without checking to make sure that they did in fact originate from where they claim to have originated.

One of the reasons that spam exists is that it is cost effective for some spammers. A certain small percentage of people who receive spam, respond to it. Such responses encourage further spamming. So, we need to educate people about the pitfalls of responding to unsolicited commercial emails (not all emails are commercial though). People are increasingly concerned about the dangerous email messages being delivered to the inboxes of youth. More than 80 percent of children who use e-mail receive inappropriate spam every day, and of all children who use e-mail, 47 percent receive spam that links to x-rated Web sites on a daily basis [23]. Technology alone cannot solve this problem. A coordinated approach that includes technological innovation, industry self-regulation, consumer education, effective legislation, and enforcement of spam and fraud laws is required.

Apart from the security issues, we cannot deny the fact that email has brought a lot of convenience to our life. It has changed the way people communicate. People of every age are using email as their preferred means of communication and the number of users is increasing everyday. Because of the vast interest in this communication medium, CNP explores the possibility to use this medium for various functions other than just simple messaging.

1.3 Outline

This chapter talks about the goal of CNP and discusses the motivation behind this work. In chapter 2, we review some of the research that has been done to address the security issues in email communication system with their shortcomings, and how CNP can improve the situation. We also discuss how email is being used beyond simple messaging. Chapter 3 describes the security, social, and economic impact of email system at present.

In chapter 4, we discuss CNP in detail, and how we can achieve improvements in email through better security and more balanced communication between sender and receiver. We have showed security improvements by presenting a few scenarios. We have also described how an email client with CNP features, i.e., Correspondence Negotiation Agent (CNA) can act as an electronic secretary by automating some of our email responses. At the end of chapter 4, we briefly address the user interface issue of CNA.

In chapter 5, we describe the basic email architecture and provide the architecture of CNP by implementing CNA, which is consisted of three main components: Authenticator, Negotiator, and eSecretary. We also discuss the implementation of these three components by mapping them to three classes. We introduce the JMail email client, which we have extended to add CNP features. A summary of classes relevant to CNP features is given at the end of the chapter.

In chapter 6, we conclude that it is possible to implement the protocol easily extending an existing email client. We compare the number of communication between CNP and non-CNP implementation of email clients. We show that our implementation is inter-operable with other Mail User Agents (MUA), and it is also platform independent.

2 RELATED WORKS

2.1 Overview

The lack of security in email, and the presence of an imbalance between sender and receiver prompted attention of the research community. As a result, there have been fair amount of research done to resolve the whole spam problem technically, such as, filtering, checking headers, blacklist/whitelist, examining contents, inclusion of confirmation step (challenge/response) by the sender, etc. Moreover, countries have even spelled out laws to stop spam. The CAN-SPAM Act is one such law that establishes various requirements for sending commercial emails and penalties for senders who are in violation of this law [29]. This chapter discusses the techniques and measures that have been taken to prevent unsolicited emails along with their shortcomings, and how these initiatives are making email communication more reliable. In this chapter, we also explain how email is used for various other services to make it more convenient and meaningful to users.

2.2 Technical Initiatives

The realization of the danger of the spam problem has prompted programmers and researchers to develop alternative and technological solutions for electronic communication. This section discusses the technological initiatives that have been taken to counter spam and the effectiveness of those measures.

2.2.1 Filtering

The most widely used anti-spam technologies employed today are based on heuristic filtering techniques that check headers and bodies of e-mail messages for key words or phrases that indicate spam. Because of the problems of both false positives and false negatives, such heuristic filtering can only be a partial solution. Email service providers such as hotmail and yahoo maintain a separate folder ("Junk E-Mail", "Bulk"), where the spam messages are saved for a certain duration. Thus, it provides the user with the opportunity to reclassify email as not to be spam if it is placed into that folder incorrectly. So, it does not help in terms of saving user's time. More importantly, filtering is only a stopgap measure that may be overcome by new bulk e-mailing strategy and technology. For example, spammers may acquire the most popular anti-spam filter software, and use it to design spam messages that make it through the filters. Programs to automate this process are sure to be developed. Even when novel probabilistic techniques (e.g. Bayesian filter) have been suggested [31], possible countermeasures have been quickly identified [IETF discussion list]. Filtering is also performed based on whitelists and blacklists set by the user. But, it is not difficult to spoof whitelisted addresses. Likewise, with many companies providing free email addresses, it is very easy to get new email address very quickly if one address gets blacklisted.

Distributed, collaborative, spam detection and filtering technique is used to stop spam in Vipul's Razor [35]. Since some spammers typically send identical messages to hundreds of people, once it is reported by one receiver, everyone else will automatically block it. Through user contribution, it establishes a distributed and constantly updated catalogue of spam in propagation that is consulted by email clients to filter out known spam. User input/report is validated through reputation assignments based on consensus report. However, the mechanism does not work in real time. Spammers move so quickly that by the time someone reports more people will be affected. Moreover, with millions of people using email and differences in defining spam, the message that is spam to one, may not be spam to someone else.

2.2.2 Sender Authentication

Theoretically, sender authentication through digital signature technology (e.g., PGP signatures) could address the problem. However, this approach suffers from a chicken-and-the-egg problem. It will not become effective until it is widely adopted; it will not be widely adopted until it has proven effective. The "incremental adoption problem" [10] is the key challenge for anti-spam technologies. Sender Policy Framework (SPF) proposed by some within the Anti Spam Research Group (ASRG), is another approach to fight against address forgery [12]. The Internet uses DNS (Domain Name System) to resolve domain names into IP addresses. DNS is also used to direct requests for different services, such as email and web servers. For each domain, an MX[2] (Mail Exchanger) record must exist. SPF publishes "reverse mail exchanger" records in DNS that tells which machines send email from the domain. The recipient of the e-mail can then check these records to ensure that e-mail is coming from a

[2] An MX record tells the email sender where the target server of receiving mail is located.

“trusted” sender from this domain. SPF allows the administrator of an Internet domain to specify which machines are authorized to transmit e-mail from that domain. SPF makes it more difficult for spammers to send spam, because if they simply forge a "From" address from an address that implements SPF, receivers with SPF implementation will ignore the e-mail [12]. If a spammer legitimately has an account in that domain, or he is the owner of the domain, they can still send e-mail. This is a real problem because there could be a massive growth in the registration of one-way domains by spammers since it just costs as low as $5/year to register a domain. SPF along with whitelists could be more effective. However, it takes away the responsibility from the legitimate owner of the individual address and puts the control solely into the hands of the domain owner. So, some freedom lost for security. Lyon and Wong have suggested to display both author and sender information to receiver [11]. Having both sender and mail-form header on display in the email client, receiver will know if the sender will receive the email if a reply is sent. It may be useful to prevent phishing attempts. Microsoft Outlook already does this by showing “from X on behalf of Y”. This could be an add-on feature as it can not alone stop unwanted email to get through to the user’s inbox.

2.2.3 Challenge - Response

Another promising approach to spam reduction is to use the idea of a sender confirmation step (challenge/response) when e-mail from a new correspondent is received. Although Hoffman and Crocker reported this as one potential solution in their 1998 survey [32], they cited concerns about "very high" potential for information loss because legitimate senders would not bother to confirm, and "mixed" success in practice because bulk e-mailers would counter with legitimate return addresses and auto responders. If designed poorly, C/R system can generate unwanted and redundant email messages. Templeton proposed some principles to consider while designing C/R system [3]. Lately, a great number of projects and products (Active Spam Killer, Tagged Message Delivery Agent, oSpam among others) have employed variations on the sender confirmation concept, with initial deployments reporting considerable success.

2.3 Social and Legal Initiatives

The Technology alone would not stop spam [IETF discussion group]. We need to create consciousness of the dangers of junk mail. It would also require effective legislation, and enforcement of spam and fraud laws. Some countries have already initiated adopting laws and legislations aimed at restriction or prohibition of unsolicited bulk mailing of either commercial or non-commercial contents. The Federal Trade Commission (FTC) passed a law called "The CAN-SPAM Act" to prevent email abuses [29]. The law became effective January 1, 2004. It bans false or misleading header information, i.e. "From", "To", and routing information must be accurate. It also prohibits deceptive subject lines in the email. The law requires that there must be an opt-out method mentioned in the email. In cases of commercial email, it must be identified as an advertisement and include sender's valid physical postal address. The law also spelled out penalties for violators. The European Union also passed a digital privacy law to stem the tide of spams. The rules require companies to gain consent before sending e-mails and introduce a ban on the use of spam throughout the EU. The United Kingdom has made spam a criminal offence to try to stop the flood of unsolicited messages. Under the new law, spammers could be fined £5,000 in a magistrate's court or an unlimited penalty from a jury [BBC News - Sep 18, 2003]. Several other countries have also taken similar initiatives.

But it is not easy to enforce these laws in cases where the emails are coming from countries where there is no such law. So, it would require international cooperation. Without such cooperation, it would be hard to hold the violators accountable and bring them to justice if they are sending spams from other countries. Moreover, since there is no way to authenticate the sender's email address in the electronic communication at present, it is not always possible to determine the actual senders of emails which are in violation of anti-spam laws.

Some have proposed that a certain cost must be imposed to send email. Among others, Bill Gates of Microsoft is suggesting that we start buying stamps to send emails [38]. It will be similar to postal service with very minimum cost, perhaps a penny for a message. Many Internet analysts worry, though, that turning e-mail into an economic commodity would undermine its value in democratizing communication. Moreover, innocent users may end up paying by becoming victims of zombies and spoofing. So, others have suggested that instead of actual cash, senders need to devote few seconds of computing time, which could be solving a math puzzle. Because time is money, and spammers would presumably have to buy many more machines to solve enough puzzles.

The open-source software Hashcash [37], available since about 1997, takes a similar approach and has been incorporated into other spam-fighting tools including Camram (CAMpaign for ReAl Mail) and Spam Assassin. It requires that the sender includes "X-Hashcash" header with hashcash stamp, which takes some time to generate. Hashcash only slows the number of mails the spammer can send (a separate stamp is required for each individual recipient) but does not stop them from sending emails.

2.4 Usage of Email

The usage of email is as individual as the users. People are using it for different reasons to meet their needs. An increasing body of literature points to the use of email (email client) as more than a simple messaging service [16, 17, 18, 19, 20, 34]. Email has transformed into a central place from which work is received, managed and delegated within organizations [17]. It serves as a repository of working information that need to be completed. So, Bellotti showed how email can be used as task management system [17]. Email is no longer being used just as a single user application; rather the same inbox is shared in collaboration among members in a group. Shared mailbox provides a convenient way to work in collaboration (e.g. between secretary and manager) by placing emails in various folders, which can represent actions or reminder [18, 19]. It can also serve as a single point-of-contact, e.g. a group of employees respond to customers' enquiry sharing the same mailbox and using same "From" address [18]. The ability to place annotations in email messages can be helpful, and serve as reminders for user much the same way that physical notes attached to documents [19].

Email is already being used as an auto responder, e.g. with vacation messages. There are many programs currently in use today that automatically respond to emails. The automatic responses via emails can provide timely notices to senders to inform them that the messages would not be read or acted on immediately, e.g. “out of office” or “vacation” messages. Similarly, the concept is used for “change of address” notification to inform/advise senders to change the address (TrueSuite). Many mail filtering programs (SpamBouncer) send automatic responses to senders about any presence of viruses or worms in the incoming emails. Email-based information service is another example of automatic email response, where requests are received through email and responses are issued (e.g. mailing list subscription requests). If automatic response to email is not designed properly, it could lead to a number of useless, unwanted, or redundant responses resulting in mail loops or denial-of-service attacks.

Because of the preference for email communication and rapid growth of using instant messaging (IM) within businesses and organizations, many have suggested to integrate IM or online-chat capabilities into email tools [19, 20, 34]. With the ability to view the sender’s online status, the receiver can initiate an IM or chat session instead of writing more email messages based on the urgency of communication. The chat transcript can eventually be saved at the end of the conversation [19]. IM feature included within the email tool, adds synchronous communication capability for users to current email system.

2.5 Improvement by CNP

The goal of CNP is to leverage and augment capabilities provided by current Mail User Agent (MUA). The processing of email has become a major time sink of our regular activities. So, we view that CNP can enable services to users through an electronic secretary by sending responses to certain emails on behalf of the user where possible. This can save user's time and improve response time. In order to increase security and prevent unwanted emails, some senders may have to negotiate through CNP to have their messages posted in the receiver's inbox. It will try to make sure that receivers receive emails, which they desire, and they do not have to receive anything that senders send. Therefore, the communication between senders and receivers will be more balanced. CNP increases email response time utilizing auto-response feature, e.g. auto response on availability taking information from user's personal calendar. While designing the protocol and implementing CNA, efforts has been given to make sure that it is usable both with the MUAs that adopt CNP and the MUAs that do not. In Chapter 4, we discuss in detail how CNP increases security of current electronic communication and makes the email experience more attractive and adds more services integrated with the email tool.

3 EMAIL COMMUNICATION TODAY

3.1 Overview

So many emails including spam arrive each day that many users are overwhelmed by the volume, missing important messages, responding late, forgetting to follow up and spending lots of time on rote email handling tasks. In this chapter we discuss the current security threats posed by emails, and social and economic impact of spam. We also discuss how email has evolved over time and met users' needs serving many different purposes.

3.2 Security Concerns

Email poses quite a number of security threats to the internet community today, such as spoofing, phishing, spreading worms/viruses, etc. Most unwanted email contains headers that lie about the origin of the mail. One of the most evident problems with current Internet mail protocols [6] is the lack of any sort of authentication with regards to the sender's identity. This shortcoming, i.e. the lack of sender's address/identity validation allows spammers to send spoofing messages and phishing scams. Spammers can even use this vulnerability to send viruses or worms by appearing as recognized sender to recipient. It becomes very difficult or in some cases impossible for the law enforcement agencies to determine who actually has sent the fraudulent email. This section discusses some of the security issues in detail, which are commonly used by spammers today.

3.2.1 Spoofing

E-mail domain spoofing involves forging a sender's address on e-mail messages. It can be used by malicious individuals to mislead e-mail recipients into reading and responding to deceptive mail. These phony messages can jeopardize the online privacy and safety of consumers, and “damage the reputation of the companies purported to have sent the messages” [11]. Email spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information, e.g. passwords. In the internet community, this is referred as phishing. Spoofing makes it difficult for law enforcement agency to find the actual sender of a fraudulent email.

3.2.2 Phishing

Spoofed e-mail often contains phishing scams. In such ploys, a spammer, posing as a trusted party such as a bank or reputable online vendor, sends millions of e-mail messages directing recipients to Web sites that appear to be official but are in reality scams. “Visitors to these fraudulent Web sites are asked to disclose personal information, such as credit card numbers, or to purchase counterfeit or pirated products” [11]. It could damage the reputation of the company/organization, whose email and website have been forged.

3.2.3 Email Worms

Worms can be distributed via email. A worm is a self-propagating malicious code unit that can automatically distribute itself from one computer to another through network connections. A worm can take harmful action, such as consuming network or local system resources, possibly causing a denial of service attack. It can also keep sending emails to addresses listed in the victim's address book.

3.2.4 Email Viruses

Viruses can also be distributed through email. Like a worm, a virus is a chunk of code written with the express intention of replicating itself. However, a virus does not spread from computer to computer directly, but by attaching itself to a host program. The host program could be the victim's email client, which would send emails with the viruses to addresses listed in the address book. It may also damage hardware, software, or data. Email-distributed viruses that use spoofing, such the "Klez" or "Sobig" virus, take a random name from the infected person's hard disk and send email themselves out as if they were from that randomly chosen address. Recipients of these viruses are therefore misled as to the address from which they were sent, and as a result, may end up complaining to, or alerting the wrong person. Thus, users of uninfected computers may be wrongly informed that they have, and have been distributing a virus.

3.2.5 Zombies

Zombies are computers that have been infected or hacked and turned into a spamming machine, sending out spam, and probably viruses, with a victim's email from infected computers with the owner's IP address. It could be very hard to convince some of the law enforcement agencies that the owner did not know that his/her computer was a zombie and that s/he is not responsible for the spam.

3.3 Social and Economic Concerns

Spam accounts for more than half of all email traffic. More than 80 percent of children who use e-mail receive inappropriate spam every day and of all children who use e-mail, 47 percent receive spam that links to x-rated Web sites on a daily basis [Symantec News Release, 2003]. Out of the 31 billion emails sent per day, 2.5 billion are pornographic (totaling four pornographic emails per day, per user) [Spam Filter Review, Q1, 2003].

The unsolicited e-mail known as spam is responsible for nearly US$20 billion in lost time and expenses worldwide [Forrester Research, 12/03]. Spam cost U.S. businesses $10 billion to $13 billion in 2003. [Ferris Research, 11/03]. WindowsITPro reported that over 80% of US email is spam. It cost European business nearly $3B in lost productivity in 2002 [BBC News, July 15, 2003]. Russia loses up to $200M USD because of spam every year [33].

3.4 Usage of Email

Email provides convenient, time-saving communication with family members, friends, co-workers, partners and customers. It has become an essential component of business today. In addition to traditional letters, email now consists of invitations, greetings, receipts, transactions, discussions, conversations, tasks, newsletters, etc. Many companies have started to send bills via email instead of postal mail. People use email to schedule meetings. Politicians have started to use email for their campaigns. Emails are used intensively for distance education courses. Students can submit their assignments by email and can receive their grades back through email. Students can even get their questions answered by email. Potential customers can ask for product information via email. Similarly, businesses can promote new products to their existing customers using email, which turns out to be much cost saving compare to postal mail. Recruiters accept resumes via email too. It allows job-seekers to send hundreds of job applications with minimum effort. Companies send “stock alert” to clients via emails.

4 CORRESPONDENCE NEGOTIATION PROTOCOL

4.1 Overview

In this chapter, we discuss the Correspondence Negotiation Protocol in detail and the improvements that we can achieve on email communication. CNP focuses on the idea of giving more control/power to recipients than what current email system can offer. It has been designed considering security improvement and balanced communication, and efficient usage of email. We have also considered better organization and visualization schemes for the email client - CNA. This chapter has been divided into three main sections, i.e. security improvement, improved usage of email, and a brief discussion on efficient organization and visualization of the email client.

4.2 Security Improvement

CNP uses blacklist, whitelist along with challenge/response mechanisms to address various security threats posed by email communication today.

4.2.1 Blacklisting

Any email, where the sender's address is listed in this list will be deleted. If a domain is black listed, emails coming from addresses within that domain will be deleted. IP addresses can be black listed as well.

4.2.2 Whitelisting

Generally, a whitelist is a list of sender ids, for whom email is automatically delivered to the recipient. An email address will be automatically added to the whitelist when an email is sent to a new recipient (not whitelisted) [2, 3]. The same approach will be taken with forward, "CC" or "BCC" addresses. The whitelist will contain the sender's email address (could be more than one), sender's MUA (could be more than one) and attachment file acceptance information. Only whitelisted senders' emails satisfying all the conditions will be delivered to the inbox. Apart from matching the email address, the email should be generated/sent using a known/approved MUA (that matches with the MUA listed in the whitelist) of the sender and in cases where emails contain attachments; sender should respond to a challenge to confirm the attachment file before it could be posted in the recipient's inbox. When an email address is added to the whitelist because the user (s/he is the sender in this case), has sent an email to that address, the MUA or the client name of the destination user may not be available. The CNA will wait for the first response/email from the destination user to determine the MUA of that user. Otherwise, our CNA would issue a challenge after receiving the response from the destination user since our CNA has no information of the MUA that could be used by the destination user.

There still remains a complication when the user subscribes to a mailing-list. In this case, the mailing-list address should be whitelisted. Any email that contains the mailing-list address in "TO", "CC" or "BCC" header will pass through.

Otherwise, it is not possible to add all the subscribers of that mailing-list to the whitelist.

In another case, the user may have a business relationship with a company, which has a domain, e.g. somecompany.com. The recipient can expect to receive email from various email addresses within that domain, i.e. sales@somecompany.com, info@somecompany.com, etc. So, the whole domain can be whitelisted initially. It may not work because spammers could easily determine that domain name and forge emails to get through [2]. If the recipient starts getting email from xyz@somecompany.com, s/he can only use certain email addresses in the whitelist, i.e. valid_addresses@somecompany.com.

Using CNP, the whitelist is augmented by a challenge/response mechanism. When an email is received from a new sender, a challenge is sent to validate the email. The sender must respond to the challenge. CNP then validates the response and posts it in the inbox. The intention is to make sure that email is sent by a human. Detailed steps are shown in Appendix A. A whitelisted sender can temporarily or permanently change his/her email address and send email from a new address (not in the whitelist). The new address must be confirmed by responding to AddressChangeQuery. The response will come from the old email address. Appendix B describes the steps in detail.

4.2.3 Anti-spoofing

Email spoofing refers to email that appears to have originated from one source when it was actually sent from another source. The spoofed email could appear to come from a whitelisted email address to trick the whitelist. However, it might so happen that the email is sent using a different MUA (not in the whitelist). Spoofed emails generally contain return-paths different than the forged sender address. CNA displays return-path information along with sender and subject. This mechanism alone does not prevent spoofed emails being posted in the inbox. Before posting to the inbox CNA checks MUA of the sender and validates it against the one in whitelist. Email that is sent using a different MUA (not listed in whitelist) will receive a challenge. Unless a valid response is received, CNA will not post the email to user's inbox. Appendix C describes the flow of emails, i.e. challenges, responses and validation process.

4.2.4 Sender Address Forgery Prevention

The anti-spoofing mechanism discussed above (4.2.3) cannot alone solve the problem. A spammer can trick the sender MUA information in the email header. Incorporating SPF with CNP will make sure that spammers will not be able to send email by just forging "From" address from an address that implements SFP. SPF supported receiving MTA will check/authenticate if the sender SMTP client is authorized to send email using the "From" address specified in the email header [11,12]. Once CNA retrieves the message from the receiving MTA, it can then decide what to do with the message based on the answer received from the authentication [11].

4.2.5 Worm/Virus Prevention

Worms and viruses are usually distributed via email attachments. The sender must confirm the attachment file before it will be posted to user's inbox. A CNA issues a challenge when it receives an email with an attachment. The sender will then have to respond to the challenge. With this mechanism, the sender will be able to know if his/her computer has been infected by a virus or attacked by zombies, which is sending email with attachment (most likely with virus) to emails listed in the address book. Detail on flow of emails can be found in Appendix D. The user can configure the attachment confirmation/validation process as to whether CNA should send a challenge for all type of attachment files or certain file types (i.e. .exe, .scr, .zip, etc.). It can also be customized based on senders, e.g. the user may decide not to issue a challenge if an attachment has come from his/her superior or a specified individual.

4.3 Improved Usage

With CNP, CNA tries to increase the usability of email and make it more convenient to users. It explores various usages of e-communication other than just simple messaging, i.e. information system, instant messaging, collaboration, role based, automatic interactions, threaded messages, scheduling, grouping of messages, etc.

The concept of an email-based information system is not new. This is used in mailing lists, which accept subscription requests via email and issue response automatically. People use email to get information on products and services. The response with requested information is delivered back via email written by a human. We propose that this process can be automated and it can work similar to a telephone information system. CNA can provide options to the sender, e.g. send an email with 1 for X, 2 for Y, 0 for initiating instant messaging (similar to phone – 0 to reach operator), etc. It can help reduce response time.

Scheduling meetings among co-workers can often become very cumbersome. There is a possibility that people would respond late about their availability. CNA, combined with a personal calendar can send automatic response on availability, i.e. "Yes" or "No". Thus, by reducing response time, it makes it easier for the sender to schedule meeting faster.

Having instant messaging included with CNA can be beneficial for co-workers in an organization [19, 20]. With an IM service, receiver can response to email message by email or by instant message and the conversation can be saved at the end [19]. Thus, it would be possible to initiate synchronous communication after receiving email.

Studies have revealed that about 1/3 of emails are connected via response hierarchy [38]. Responses can come from various people in different times. Related messages can go down the list and become out of sight. With message threading it is possible to connect related messages [20], i.e. combining root message along with its response and subsequent massages together. It provides a convenient way to work with connected messages. Once a message is selected, a CNA could display all related messages in another display panel [17]. It happens quite often that a new individual is required to be drawn into the communication/conversation. CNA can send all previously connected messages as a whole through threading [17], which is usually done by forwarding each of the related messages one after another. Thus, it can speed up the whole process.

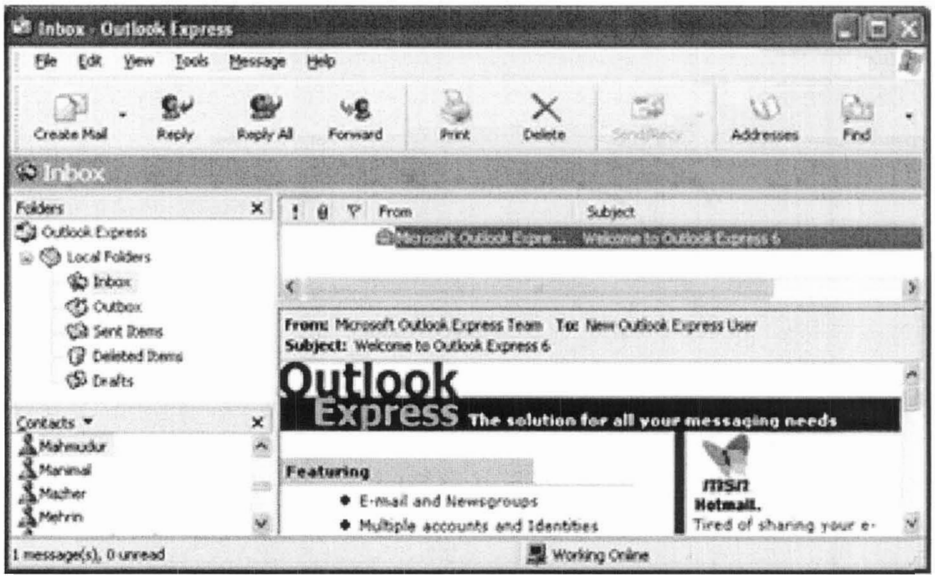
Email systems like yahoo (http://mail.yahoo.com) send reminders (by sending emails) on appointments, meetings, etc. at specific times previously set by the user. It increases the number of emails received by the user. With so many emails received each day, these reminders can go down the list and become out of sight. A CNA could display a meeting reminder using a pop-up window on the day of the meeting when it is opened for the first time that day.

CNP allows a convenient way to send "change address" notification. When email is received at the old address, the sender is sent an automatic notification about "change address" with the new email address. CNA at the other/receiving end then updates the whitelist accordingly. The receiving CNA also forwards the email to new address. Detailed flow of emails is discussed in appendix E.

CNP uses a RuleTable that allows user to set actions based on various conditions. There are two different actions: a) reply and b) forward. People frequently receive certain emails, which may not require their direct attention. An auto "reply" can be set to direct senders to online resources. People also receive various enquiries in emails for which the sender should contact someone else. In such cases, email can be forwarded to the appropriate individual using auto "forward". For example, course instructors can forward student enquiries to teaching assistants. Users can set rules on the attachment file type, i.e., if the user receives a file with the .doc extension as an email attachment, with an auto "reply", the sender can be notified that s/he must send .pdf or .ps file instead.

4.4 Efficient Organization and Visualization

Considering the large volume of email received each day, it is important to have an email client with good user interface where emails can be organized efficiently. Since organization and visualization are two important aspects of any email client, we will briefly discuss these in this section. The original three pane interface (folders, email-list, preview) used in some email systems is not sufficient when it comes to organizing high volume of emails [20]. Some email systems, such as Microsoft Outlook and Hotmail includes another pane with contact list to facilitate retrieving addresses when user wants to send email to individuals in his/her contact. The user interface of typical email system is shown below.



Microsoft Outlook Expre... Welcome to Outlook Express 6

From: Microsoft Outlook Express Team To: New Outlook Express User
Subject: Welcome to Outlook Express 6

- E-mail and Newsgroups
- Multiple accounts and Identities

Tired of sharing your e-

1 message(s), 0 unread

Figure 4.1: MUA Interface of Microsoft Outlook.

With so many emails coming everyday, the list of emails (top-right panel) can grow rapidly that responses of certain email (message thread) can go out of sight. It is not very convenient or time efficient to scroll down to look for response (subsequent responses) of particular email. Therefore, we are suggesting adding another panel, which will display all messages in a thread when any message in that thread is selected [17].

The user may be interested to view all the messages that came from a particular sender in the address book or contact list. When any contact in the address book is opened, all the messages sent from that individual will be displayed.

5 CNP ARCHITECTURE AND IMPLEMENTATION

5.1 Overview

In this chapter, we discuss the architecture of both basic email communication system and that of CNP. This chapter is divided into three main sections: basic email architecture, CNA architecture, and CNP implementation.

5.2 Basic Email Architecture

Sender/user composes and sends email using an MUA, and hands over the email message to sender MTA, which acts as the outgoing mail server. The MTA then communicates with the receiver MTA and passes the message. This communication is performed using SMTP [6]. There could be many intermediate MTAs in between the sender and receiver MTAs. Once the email has arrived at the receiver MTA, the email is posted/appended to the receiver's mailbox. The software that places email into receiver's mailbox is called the Mail Delivery Agent (MDA), or Local Delivery Agent (LDA).

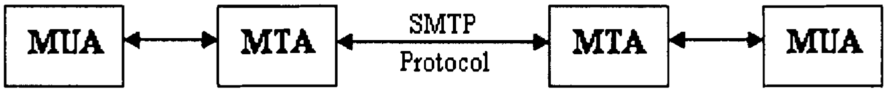


Figure 5.1: Basic Email Architecture.

Once the email reaches the destination, it can be retrieved using either Post Office Protocol (POP) [RFC 1939] or Internet Message Access Protocol (IMAP) [RFC 2060]. The receiver can use his/her MUA to read the email after retrieval.

SMTP is independent of the particular transmission subsystem. It requires only a reliable ordered data stream channel. TCP is mainly used as the underlying transport service. The basic SMTP structure can be pictured as follows:

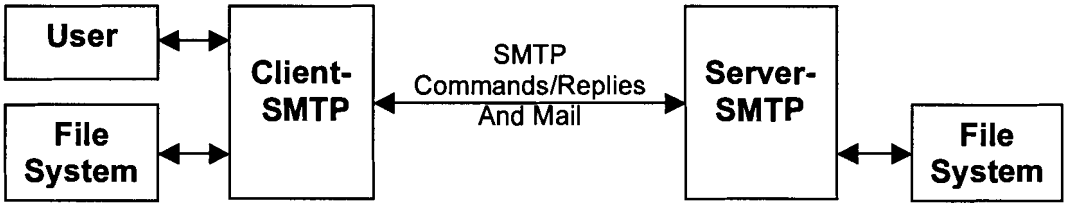


Figure 5.2: SMTP Structure [6].

SMTP has the capability to transport mail across networks, which is referred as "SMTP mail relaying". Mail can be relayed between hosts, i.e., SMTP clients/servers, which are located in different networks having dissimilar transport system. When an SMTP client has a mail to transmit, it establishes a two-way transmission channel to an SMTP server. The responsibility of an SMTP client is to transfer mail to one or more SMTP servers, or report its failure to do so.

5.3 CNA Architecture

CNA processes each message for validation. Validation criteria are set by the user. Validation can occur locally, or it may involve communication with the sender. Negotiations between sender and receiver CNAs take place. Only valid messages are posted to the receiver's inbox. We have a introduced few headers to facilitate communication between two CNAs. As shown in Figure 5.3 below, CNA acts as an interface between MUA and MTA.

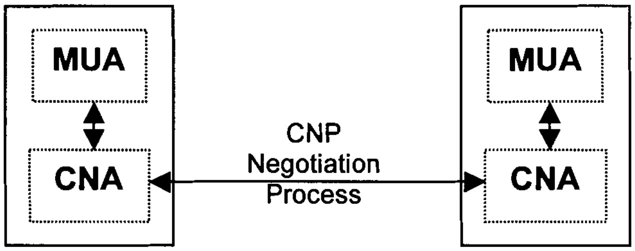


Figure 5.3: Communication Using CNP.

CNA consists of 3 main components: Authenticator, Negotiator, and eSecretary. These components interact with each other and make CNP services available to the user. Negotiator and Authenticator provide security services, whereas eSecretary aids the user in his/her daily communications.

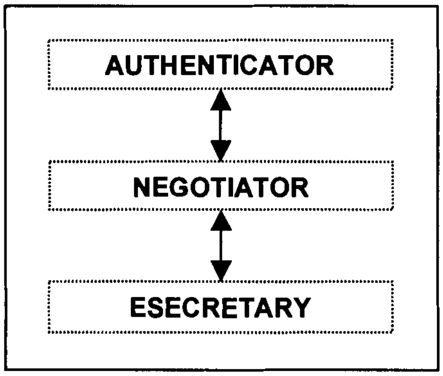


Figure 5.4: CNA Architecture/Modules.

5.3.1 Authenticator

Authenticator is one of the modules within CNA, which does the validation check on the incoming email. Negotiator asks Authenticator to perform validation check on a new email. Authenticator consults with the blacklists and whitelists, checks for virus in the attachment, and applies SPF rules in order to determine if the email received is valid, or the cause of the email being invalid. The outcome is passed back to the Negotiator afterwards.

5.3.2 Negotiator

When a new email is received, Negotiator's first task is to pass the email to Authenticator for validation. Based on the outcome, it classifies each email. After the classification, it can initiate the negotiation process by sending reply/challenge to the sender, or pass the email to eSecretary.

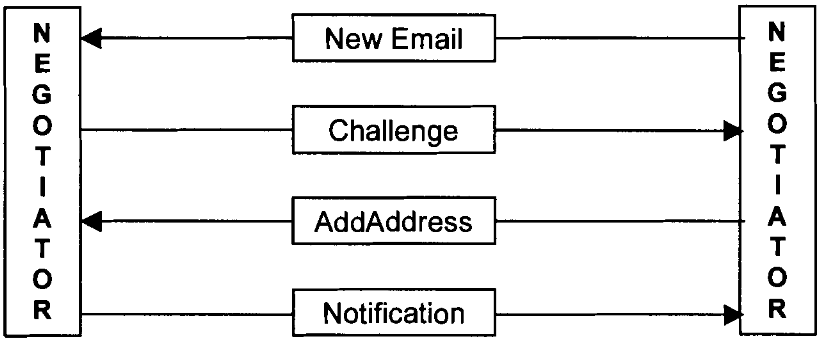


Figure 5.5: New Contact / First Time.

The Figure 5.5 above shows 2 Negotiators in negotiation process and the flow of email communications between them. Negotiator triggers this challenge when Authenticator finds that the email has come from an unknown email address (not listed in the user's whitelist). There could be three possibilities: a new valid sender who wants to initiate a communication, a known contact who has used a different/new email address, and spammer/automated spam generator sending spams. In case of the first option, the sender will have to respond to the challenge with a unique id/string (included in the challenge). For simplicity, we are using the message id of sender's initial email for the unique string. The following diagram, Figure 5.6 shows the second option and the flow of email communications among 3 Negotiators when a whitelisted sender sends an email from a new email address.

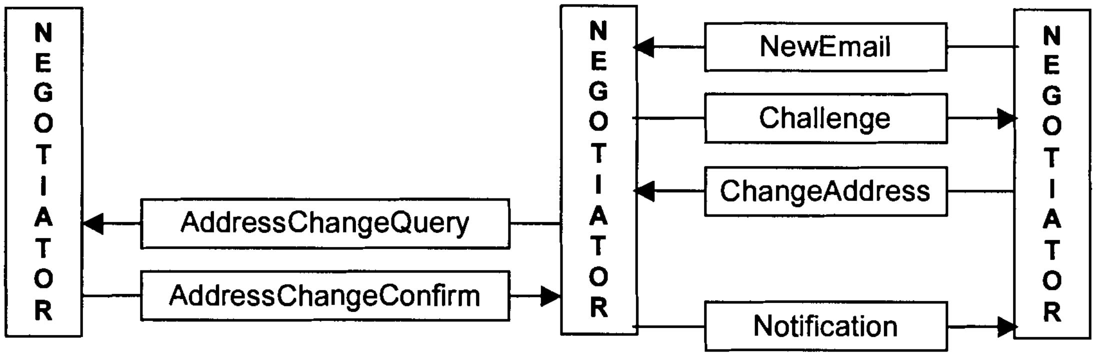


Figure 5.6: New Email Address.

The following diagram, Figure 5.7 depicts the interaction between two Negotiators showing the negotiation process when an email came from a whitelisted email address, but with an unknown MUA configuration. The new email could come from valid sender or from a spammer who forged one the whitelisted email addresses, but using a different MUA.

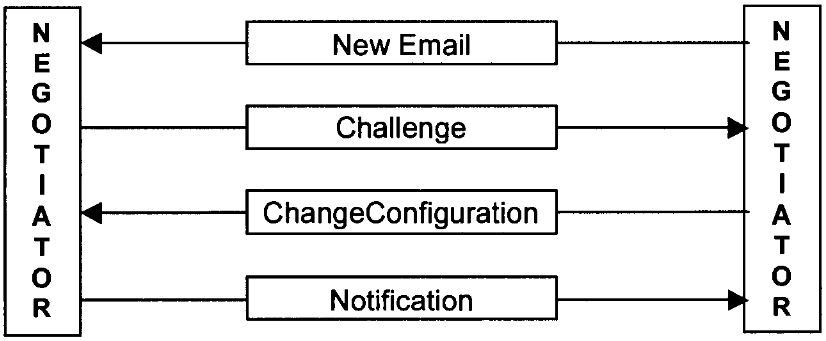


Figure 5.7: New Mail User Agent.

Once a response is received from the whitelisted sender, the response will be validated. Appropriate notification will be sent to the whitelisted sender when validation is successful, or the original message will be discarded if validation fails. We can expect that ChangeConfiguration message shown above has either been generated by CNA, or written by a human (when the sender is not using email client with CNP features).

5.3.3 E-Secretary

Once each email is processed by the Negotiator, it is passed on to the eSecretary. The eSecretary processes the email against the RuleTable, and determines if it can send a reply automatically to the sender on behalf of the user. The user can set different rules based on the sender address, subject, attachment file type, email content, etc. It may also consult the personal calendar to prompt a meeting reminder and check availability. It also sends a "change address" notification if email is sent to the old address. New emails, which require a user's attentions, are posted in the inbox at this point.

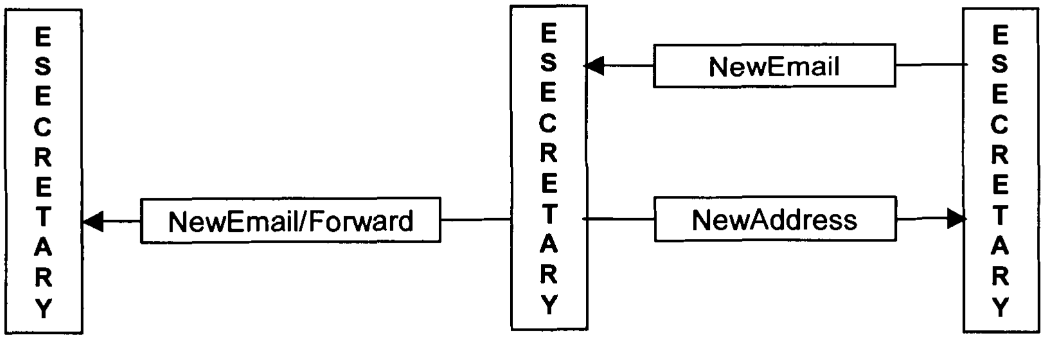


Figure 5.8: New Email Address.

The diagram above, Figure 5.8 shows the flow of messages among eSecretaries when an email came from a whitelisted sender to a user's old email address.

5.4 CNP Implementation

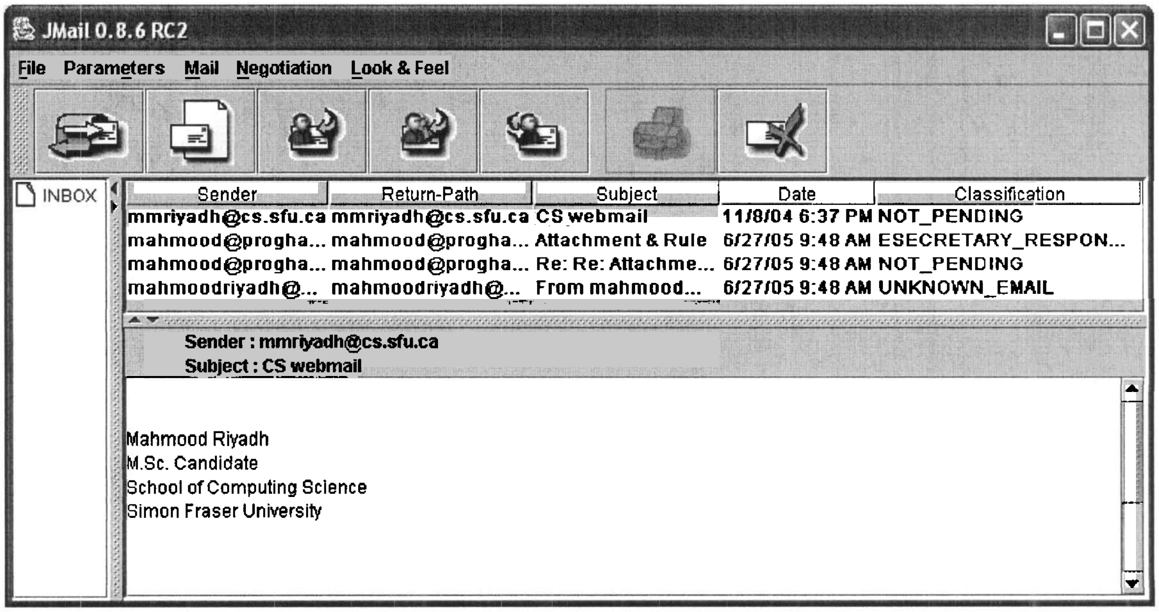
CNP features have been implemented in CNA by extending JMail [38]. JMail is an open source email client written in Java. JMail is capable of retrieving emails from both IMAP and POP3 mail servers. JMail uses a PRF-file system (Pseudo Resource Files) to store user's profile, i.e., information about the user's email account, incoming email server configurations etc. PRF-files have shorter access time than ordinary resource files, and can be used cross-platform. All the information is written in XML format. Classes from javax.xml.parsers package are used to parse the XML document. Language specific properties files have been used with the ResourceBundle class to provide multi-language support.

The three components of CNA mentioned in section 5.3 correspond to 3 main classes: Authenticator, Negotiator, and eSecretary. Apart from these three, few other new classes have been implemented and some of the classes of JMail have been modified so that CNP features could be added. Some of those most relevant classes are summarized towards the end of this section.

Authenticator performs a validation check using *isInBlacklist()*, *isInWhitelist()*, *isMUAWhitelisted()*, and *getFileAttachmentStatus()*. A new email is deleted if *isInBlacklist()* returns true, i.e., the sender's email is listed in user's blacklist. *isInWhitelist()* checks if the sender's email address is listed in the user's whitelist. Similarly, *isMUAWhitelisted()* determines if the email has been sent using an MUA, which is known to the user. At this point, the email can be further authenticated using the Sender Address Forgery Prevention mechanism discussed in section 4.2.4 applying SPF rules. This requires the incoming mail server (MTA) to implement SPF and the domain administrator to publish authorized host information. As it has not been officially standardized by the IETF community yet, it has not been implemented in CNA at this time.

The Negotiator classifies each email after Authenticator finishes its tasks. In order to classify emails, Negotiator checks various headers proposed in the CNP protocol (see appendices). These headers are not standard, and because of that, they may not be used by other mail clients. Therefore, we have also made CNA capable of parsing the email body/content using classes in the Java regular expression package: java.util.regex. For example, in "New Email Address Scenario" (Appendix B), CNP uses X-AddressChangeQuery header to authenticate the sender's claim (the email address has been changed) by sending an email to old email address. Now, if the response comes from an email client that implements CNP features, the email client will recognize the X-AddressChangeQuery header, and the response will contain X-AddressChangeConfirmed header. This response will be generated by the email client. On the other hand, if the response is written by a human (who is using email client that does not support CNP), his/her response would be checked based on the email content. In this case, response will contain "AddressChangeConfirmed(pjb@oldISP.com, paul@newISP.com)" in the body. In such case, the CNA will parse the email content.

The following diagram shows list of emails, and their classifications in the CNP email client. It also displays the "return-path" of the email message. Thus, the user knows who will receive the message if a "reply" to a message is sent.



Sender	Return-Path	Subject	Date	Classification
mmriyadh@cs.sfu.ca	mmriyadh@cs.sfu.ca	CS webmail	11/8/04 6:37 PM	NOT_PENDING
mahmood@progha...	mahmood@progha...	Attachment & Rule	6/27/05 9:48 AM	ESECRETARY_RESPON...
mahmood@progha...	mahmood@progha...	Re: Re: Attachme...	6/27/05 9:48 AM	NOT_PENDING
mahmoodriyadh@...	mahmoodriyadh@...	From mahmood...	6/27/05 9:48 AM	UNKNOWN_EMAIL

Sender : mmriyadh@cs.sfu.ca
Subject : CS webmail

Mahmood Riyadh
M.Sc. Candidate
School of Computing Science
Simon Fraser University

Figure 5.9: CNA Screenshot.

The following table summarizes various classification values with description, and corresponding methods, which are executed by Negotiator. Methods specified in the table perform the negotiation process.

Classification Value	Description	Methods

UNKNOWN_EMAIL	Email came from an unknown address, possibly new contact, or old contact with new address.	*sendChallenge()*
		sendReplyToAddAddress()

CHANGE_EMAIL	Email came from an old contact, but with a new email address.	*sendChangeAddrQuery()*
		sendChangeAddrConfirmed()
		sendChangeAddrConfirmNotify()

UNKNOWN_MUA	Email came from a known address, but the sender's MUA did not match.	*sendChallengeAuthenticity()*
		sendReplyToChallengeAuthenticity()
		sendReplyToConfirmedConfig()

INVALID_ATTACHMENT	Email came from a known email address with known MUA, but the email contains attachment file that requires confirmation from the sender.	*sendChallengeForAttachment()*
		sendReplyToAttachmentConfirm()

NOT_PENDING	Email passed the validation test by Authenticator. Email is further processed by eSecretary.	*Methods are executed by* eSecretary.

Table 5.1: Classification Table.

Each method shown in the third column of the table (Table 5.1) above correspondences to email message sent by the Negotiator.

eSecretary processes email, which has been classified as NOT_PENDING by Negotiator. At this point, it executes the *applyRules()* method, and depending on information in the RuleTable, auto*Reply()* and/or *autoForward()* methods are/is invoked. When a new email is received at the old email address, eSecretary notifies the sender about the new address and forwards the email to user's new address by executing both auto*Reply()* and *autoForward()* respectively (Appendix E). eSecretary reclassifies NOT_PENDING emails into ESECRETARY_RESPONDED after sending automatic response. Thus, the user knows eSecretary responded to which emails.

It is very important to ensure that CNP does not allow redundant challenges, which can result in an infinite challenge/response loop. While Negotiator is in negotiation process with a sender, it must not issue a new challenge if a new email is received from the same sender. The Negotiator checks if there is any pending message from the sender before issuing a challenge. Whenever the user sends email to a new address (i.e., not in user's whitelist), the address is added to the whitelist. Thus, it prevents CNA from issuing a challenge to a response of the user's own message.

The following table summarizes few of the classes most relevant to CNP features. It also specifies if the classes are newly implemented or modified:

Class Name	Implementation	Description
BlackListEntry	Implemented	Contains the blacklisted email address or the domain name.
WhiteListEntry	Implemented	Contains information of the whitelisted conact, i.e., email, MUA, and fileAttachmentStatus.
Rule	Implemented	Mainly contains condition, action, and actionText.
EmailEntry	Implemented	After classification by the Authenticator, new email information is kept by creating an instance of this type. messageID, inboxStatus, senderEmail, senderMUA, pendingStatus, and pendingType are its main attributes.
CreateProfile	Modified	This is used when the client cannot find any prf file, i.e., the user configuration file. It creates new Profile.
Profile	Modified	When the email client is started, it loads the user information by parsing the prf file and updates the file at the end.
JMailWindow	Modified	Provides the menu items and contains MainPanel.
MainPanel	Modified	Provides main GUI components. Emails are processed here by calling various methods of Authenticator, Negotiator, and eSecretary.
SortableTable	Modified	It is used in MainPanel to display the list of messages. It has been modified to use Vector instead of array.

Table 5.2: Class Summary.

The original JMail software had 32 class files in total. An additional 19 classes have been implemented in order to add CNP features. Approximately, 4500 lines of Java code (including inline comments) have been written to implement CNA. Java version 1.4 or higher is required along with JavaBeans Activation Framework: jaf-1.0.2 and JavaMail API: javamail-1.3.1. CNP has been tested running on Windows 2000/XP, Red Hat Enterprise Linux, and Sun Solaris.

6 CONCLUSION

6.1 Summary

We have shown how CNP features can be implemented by extending an existing email client, i.e., JMail. By using a Platform independent programming language, i.e., Java, we have made it highly portable. Apart from testing communications among CNAs, we have also tested CNA with other widely used email clients, such as, Microsoft Outlook, Eudora, and a web based email client – SFU Webmail. Therefore, CNP can be used to maintain communication with people who are using different email clients, with no CNP features. We have also shown that email clients can act as an electronic secretary by setting various rules and automating email correspondence.

We have mainly used the challenge/response approach (introduced in section 2.2.3) in order to improve security and offer more balanced email communication. With challenge/response, we can get more communications when authentication is required. This could result in delay in getting the message posted to the inbox. Therefore, in order to achieve security and balance, we are accepting little delay. The delay can be kept minimal if both senders and receivers are using CNP. For example, in the "anti-spoof" scenario, it will require less time if the response to challenge is CNA generated instead of human written. Moreover, a message can get lost if the sender decides not to respond to the challenge. In cases of, "new address" (Appendix B) and "address change"

(Appendix E), in order to achieve the benefit of CNP there needs to be a forwarding/replying mechanism offered by the old email address provider. The “new contact” scenario (Appendix A) can be vulnerable to abuse. Spammers can set auto-responders to respond to challenges specified in this scenario. However, every time the initial email has to come from a different address since CNP does not allow sending challenges to subsequent emails from the same sender. The following table compares mail user agents with and without CNP features in terms of the number of communication in each scenario:

Scenario Name	Number of Communication			
	Non-CNP Implementation	CNP Implementation		
		Total	Automatic	
			One CNA	All CNA
New Contact	1	4	2	2
New Address	1	6	3	4
Anti-spoof	1	4	2	3
Email Attachment	1	4	2	2
Change Address	1	3	2	2

Table 6.1: Number of Communication Comparison.

As shown in Table 6.1 above, there are more communications in the CNP implementation (third column). However, most of the additional messages are automatically generated by CNA. Thus, it requires minimal human involvement. Second column shows that there is only 1 email communication without CNP implementation, but the recipient has to deal with the email even if it is a spam (according to the recipient). Column 4 and 5 show that there is further reduction

(New Address, Anti-spoof) in human involvement if both sender and receiver are using CNP. We keep record of each challenge sent. This way, we make sure that CNP does not allow redundant challenges to subsequent emails from the senders to whom challenge has already been sent.

The work presented in this project is an initial study of Correspondence Negotiation Protocol. This provides a base for future studies. More work is required to investigate the feasibility and effectiveness of this protocol. This may include testing CNA with some spam generators, using it for daily email communication over a period of time, getting feedbacks from users, etc. The duration of waiting period, (i.e., how long CNA should wait for response of a challenge before deleting the original message) also needs to be addressed. The issue of mailing-list is another area that needs to be explored.

6.2 Future Work

Not all the ideas discussed in Chapter 4 have been implemented and completion of those ideas could be the next step. One possible extension would be to make it capable of performing task scheduling. CNA can respond to an availability request if it has access to the personal calendar of the user. It will send availability information after validating the sender. A precise model is first required to determine message format, header requirement, calendaring system, etc.

Inclusion of Instant Messaging capability will present users with another form of communication capability along with email. CNA users should know each others' online status so that the recipient can initiate a chat session with the sender after receiving an email. The implementation of organizing related messages based on threads could be another interesting addition. It will require changes in the user interface of MUA so that connected messages can be displayed properly, e.g., hierarchically from the root message.

Shifting some of the tasks to the MTA level can make CNP perform better. For example, MTA can delete messages based on blacklist information set by the user. The deletion can be executed by the Mail/Local Delivery Agent before it posts the messages to user's mailbox. As a result, CNA will not have to process blacklisted messages.

APPENDIX A

New Contact Scenario

The following scenario illustrates basic challenge-response interaction, featuring X-ConfirmedAddressAdded header. When an unknown person tries to initiate email correspondence, a challenge is sent to verify the legitimacy.

1. Initiation: Paul wants to contact prof Rob whom he met in a seminar and sends an e-mail.

Date: Thu, 29 May 2003 09:01:01
To: rob@alma_mater.edu
From: paul@newContact.com
Subject: Seminar 2003

Hi, Rob. I met you at seminar 2003 ....

2. Challenge: Rob's automated e-secretary does not recognize paul@newContact.com and issues a challenge with several potential choices.

Date: Thu, 29 May 2003 09:01:47
From: rob@alma_mater.edu
To: paul@newContact.com
Subject: Re: Seminar 2003

Rob's e-secretary here.
You've sent e-mail to Rob, but I don't recognize you.
You have several choices.
....
If this is your first email to me,
send me an email containing
AddAddress(id, paul@newContact.com).
Please, use the following(Paul's original email id)
for id:

....
If you've changed e-mail addresses,
tell me ChangeAddress(old, new)
...

3. Response: Paul notes the new contact option and responds accordingly.

```
Date: Thu, 29 May 2003 09:05:11
To: rob@alma_mater.edu
From: paul@newISP.com
Subject: Re: Seminar 2003

OK, AddAddress(id, paul@newContact.com)
```

4. Delivery Notification: Rob's e-secretary receives the address confirmation and accepts it. The e-secretary adds it to Rob's address book and confirms delivery of the original message. Elapsed time: 7 minutes.

```
Date: Thu, 29 May 2003 09:05:56
From: rob@alma_mater.edu
To: pjb@oldISP.com
Subject: Re: Seminar 2003
X-ConfirmedAddressAdded: addedContact(id, paul@newContact.com) **

Rob's e-secretary here.
I have confirmed your address and have added to
Rob's address book accordingly. Your original
message with subject "Seminar 2003" has been
posted to Rob's inbox.
```

Notes

The message id is used here as a unique code to verify the legitimacy of the email. It can be used for future correspondence to prevent sender's email being forged.

APPENDIX B

New Email Address Scenario

The following scenario illustrates enhanced challenge-response interaction, featuring X-AddressChangeQuery and X-AddressChangeConfirmed headers.

1. Initiation: Paul wants to renew ties with an old friend and sends an e-mail.

Date: Thu, 29 May 2010 09:01:01
To: rob@alma_mater.edu
From: paul@newISP.com
Subject: Long Time, No See

Hi, Rob. It's been months ....

2. Challenge: Rob's automated e-secretary does not recognize paul@newISP.com and issues a challenge with several potential choices.

Date: Thu, 29 May 2010 09:01:47
From: rob@alma_mater.edu
To: paul@newISP.com
Subject: Re: Long Time, No See

Rob's e-secretary here.
You've sent e-mail to Rob, but
I don't recognize you. You have
several choices.
....
If you've changed e-mail addresses, tell me ChangeAddress(old,new)
...

3. Response: Paul notes the address change option and responds accordingly.

Date: Thu, 29 May 2010 09:05:11
To: rob@alma_mater.edu
From: paul@newISP.com
Subject: Re: Long Time, No See

OK, ChangeAddress(pjb@oldISP.com, paul@newISP.com)

4. Challenge 2: Rob's automated e-secretary recognizes the request for an e-mail address change and attempts to verify the change through the old address. The body of the challenge is intended to be read by a human, but a header field is also provided for machine-processing.

Date: Thu, 29 May 2010 09:05:56
From: rob@alma_mater.edu
To: pjb@oldISP.com
Subject: Address Change Query
X-AddressChangeQuery: FromTo(pjb@oldISP.com, paul@newISP.com)

Rob's e-secretary here. I have an address change request
claiming that paul@newISP.com is the new address for
pjb@oldISP.com. If this is correct please send a message
including the line:
AddressChangeConfirmed(pjb@oldISP.com, paul@newISP.com)

5. Response 2: Paul has his own e-secretary at his old address, programmed to recognize X-AddressChangeQuery headers and confirm the address change requests immediately.

Date: Thu, 29 May 2010 09:06:12
From: paul@oldISP.com
To: rob@alma_mater.edu
Subject: Re: Address Change Query
X-AddressChangeConfirmed: FromTo(pjb@oldISP.com, paul@newISP.com)

Paul's e-secretary here. This is Paul's old address.
AddressChangeConfirmed(pjb@oldISP.com, paul@newISP.com)

6. Delivery Notification: Rob's e-secretary receives the address change confirmation and accepts it. The e-secretary update Rob's address book and confirms delivery of the original message. Elapsed time: 7 minutes.

Date: Thu, 29 May 2010 09:07:42
From: rob@alma_mater.edu
To: paul@newISP.com
Subject: Re: Long Time, No See

Rob's e-secretary here.
I have confirmed your address change and have updated
Rob's address book accordingly. Your original
message with subject "Long Time, No See" has been
posted to Rob's inbox.

Notes

Security concern: if an old e-mail address is fraudulently misappropriated, this mechanism may be abused to create trust in arbitrary new e-mail addresses.

APPENDIX C

Anti-spoofing Scenario

The following scenario illustrates enhanced challenge-response interaction, featuring X-Challenge-Authenticity.

1. Initiation: Mary has changed her e-mail set up and sends a message to Rob.

```
Date: Thu, 29 May 2004 09:01:01
To: rob@alma_mater.edu
From: mary@company.com
Subject: New MUA

Hi, Rob. I've switched e-mail programs...
```

2. Challenge: Rob's automated e-secretary notices that an e-mail apparently from Mary has a different User-Agent header. Rob has configured his secretary to challenge on changes in User-Agent or originating mail server.

```
Date: Thu, 29 May 2004 09:01:47
From: rob@alma_mater.edu
To: mary@company.com
Subject: Re: New MUA
X-Challenge: ConfirmMessageAndConfiguration

Rob's e-secretary here.  I've received mail that
claims it's from you, but doesn't match your
previous e-mail configuration.  Please confirm
so that I can deliver your mail to Rob.   Send a
reply containing one of the following lines.

ChangeConfiguration - I've changed the way I send e-mail.
SetAlternateConfiguration - I may still use the old configuration.
SetTemporaryConfiguration - This is just a temporary change.

> Date: Thu, 29 May 2004 09:01:01
> To: rob@alma_mater.edu
> From: mary@company.com
> Subject: New MUA
>
```

> Hi, Rob. I've switched e-mail programs...

3. Response: Mary's new e-mail set-up includes an e-secretary that automatically confirms requests to confirm the configuration change.

Date: Thu, 29 May 2004 09:02:22
To: rob@alma_mater.edu
From: mary@company.com
Subject: Re: New MUA
X-Response: ConfirmMessageAndConfigurationChange

ChangeConfiguration - I've changed the way I send e-mail.

4. Delivery Notification: Rob's e-secretary receives the address change confirmation and accepts it. The e-secretary update Rob's database noting Mary's e-mail configuration. Elapsed time: 2 minutes.

Date: Thu, 29 May 2004 09:07242
From: rob@alma_mater.edu
To: mary@company.com
Subject: Re: New MUA

Rob's e-secretary here.
I have confirmed your new-email configuration
and updated my files accordingly. Your original
message with subject "New MUA" has been
posted to Rob's inbox.

APPENDIX D

Email Attachment Scenario

This scenario illustrates basic challenge-response interaction by email with attachment. When a Whitelisted person tries to send an email with attachment, a challenge is sent to get confirmation that the sender has indeed sent the email with attachment.

1. Initiation: Paul wants to send an email with attachment to prof. Rob. Paul is already in Rob's Whitelist.

Date: Thu, 29 May 2010 09:01:01
To: rob@alma_mater.edu
From: paul@whitelistContact.com
Subject: Email Attachment
Content-Type: multipart/mixed;

Hi, Rob. I've sent you an email attachment.

2. Challenge: Rob's automated e-secretary does not accept email with attachment from whitelisted email address without confirmation from the sender. Therefore, it issues a challenge.

Date: Thu, 29 May 2004 09:01:47
From: rob@alma_mater.edu
To: paul@whitelistContact.com
Subject: Re: Email Attachment
Content-Type: text/plain;

Rob's e-secretary here.
You've sent e-mail to Rob with attachment, but
I don't accept email attachment without confirmation. You must send me an email containing the following line.
....
AttachmentFileConfirmed(FileName).
i.e. AttachmentFileConfirmed(sample.pdf)

3. Response: Paul notes the attachment option and responds accordingly.

Date: Thu, 29 May 2004 09:05:11
To: rob@alma_mater.edu
From: paul@whitelistContact.com
Subject: Re: Email Attachment
Content-Type: text/plain;

OK, AttachmentFileConfirmed(FileName)

4. Delivery Notification: Rob's e-secretary receives the attachment notification and accepts the email with attachment, which was sent earlier. The e-secretary then confirms delivery of the original message.

Date: Thu, 29 May 2004 09:05:56
From: rob@alma_mater.edu
To: paul@whitelistContact.com
Subject: Re: Email Attachment
Content-Type: text/plain;

Rob's e-secretary here. Your original message with subject
"Email Attachment" has been posted to Rob's inbox.

Notes

With this mechanism, sender will be able to know if his/her computer has been infected by virus and became a zombie machine, which is sending email with attachment (most likely with virus) to email addresses listed in the address book.

APPENDIX E

Address Change Scenario

This scenario illustrates change of address notification, featuring X-NewAddress.

1. Initiation: Paul wants to sends an e-mail to one of his old friends who recently changed his email address.

Date: Thu, 29 May 2004 09:01:01
To: rob@oldISP.com
From: paul@whitelistContact.com
Subject: Long Time, No See

Hi, Rob. It's been months ....

2. Forwarding: Rob's automated e-secretary forwards the email to Rob's new address

Date: Thu, 29 May 2004 09:01:47
From: rob@oldISP.com
To: rob@newISP.com
Subject: fwd: Long Time, No See

The following message has been received in your old address.

Date: Thu, 29 May 2004 09:01:01
To: rob@oldISP.com
From: paul@whitelistContact.com
Subject: Re: Long Time, No See

Hi, Rob. It's been months ....

3. Notification: Rob's automated e-secretary notifies Paul about the address change.

Date: Thu, 29 May 2004 09:01:50
From: rob@oldISP.com
To: paul@whitelistContact.com
Subject: Re: Long Time, No See
X-NewAddress: NewAddress(newAddress)

Rob's e-secretary here. You've sent e-mail to Rob, but
his email address has been changed recently. Your email has been sent
to his new address. Consider the following address in future.

NewAddress(newAddress)

BIBLIOGRAPHY

[1] P. Dutta and K. M. Narayanaswami. Eliminating Spam: Protocol and Infrastructure Changes. 2003. http://www.chaoszone.org/misc/spam.html. Accessed: July 15, 2005.

[2] D. A. Wheeler. Countering Spam with Ham-Authenticated Email and the Guarded Email Protocol. 2003. http://www.dwheeler.com/guarded-email/guarded-email.html. Accessed: July 15, 2005.

[3] B. Templeton. Proper Principles for Challenge/Response Anti-spam Systems. http://www.templetons.com/brad/spam/challengeresponse.html. Accessed: July 15, 2005.

[4] E. Dean and Y. Shafranovich. Challenge/Response Interworking (CRI) Framework for Challenge / Response Email System. Internet Draft, ASRG, 2003. http://www.shaftek.org/drafts/draft-irtf-asrg-cri-00.txt. Accessed: July 15, 2005.

[5] D. Crocker, V. Schryver, and J. Levine. Technical Consideration for Spam Control Mechanism. Interner Draft, ASRG, 2003. http://www.ietf.org/internet-drafts/draft-crocker-spam-techconsider-02.txt. Accessed: July 15, 2005.

[6] J. Klensin Simple Mail Transfer Protocol. RFC-2821, 2001.

[7] P. Resnick. Internet Message Format. RFC-2822, 2001.

[8] J. Fenley. Choicelist – A Minimally Intrusive, Recipient Configurable, Authentication and Permission Granting System for Email. FTC Spam Forum, 2003.

[9] D. Martz. Spam Filtering Technique. 2002. http://www-106.ibm.com/developerworks/linux/library/l-spamf.html. Accessed: July 15, 2005.

[10] L. F. Cranor and B. A. LaMacchia. Spam! Communications of the ACM, Volume 41, Number 8, 1998, pp. 74-83.

[11] J. Lyon and M. W. Wong . Sender ID: Authenticating E-Mail, Internet Draft, 2004. http://www.ietf.org/internet-drafts/draft-lyon-senderid-core-01. Accessed: July 15, 2005.

[12] M. W. Wong and M. Lentczner. The SPF Record Format and Test Protocol. Internet Draft, 2004. http://xml.coverpages.org/draft-ietf-marid-core-03.txt. Accessed: July 15, 2005.

[13] P. Mockapetris. Domain Names - Concepts and Facilities. RFC - 1034,1987.

[14] P. Mockapetris. Domain Names - Implementation and Specification. RFC - 1035, 1987;

[15] H. Danisch. The RMX DNS RR and Method for Lightweight SMTP Sender Authorization. Internet Draft, 2004. http://ietfreport.isoc.org/idref/draft-danisch-dns-rr-smtp/. Accessed: July 15, 2005.

[16] R. Baker, N. Duarte, A. Haririnia, D. Klinesmith, H. Lee, L. Velikovich, A. Wanga, M. Westhoff, and C. Plaisant. Role Management. CSCW 2002.

[17] V. Belotti, N. Ducheneaut, Mark Howard, and I. Smith. Taskmaster: Recasting email as task management. CSCW 2002.

[18] M. Muller and D. Gruen. Collaborating within – not Through – Email: Users Reinvent a Familiar Technology. CSCW 2002.

[19] S. L. Rohall. Redesigning Email for the 21st Century. CSCW 2002.

[20] P. B. Moody. Reinventing Email. CSCW 2002.

[21] G. Venolia, C. Neustaedter. Understanding Sequence and Reply Relationships within Email Conversations: A Mixed Model Visualization. CSCW 2002.

[22] D. Fisher. Email in Social Workspace. CSCW 2002.

[23] Business Wire / Symantec. Symantec survey reveals more than 80 percent of children using e-mail receive inappropriate spam daily. Symantec News Release, 2003.

[24] P. Bruening. Technological Responses to the Problem of Spam: Preserving Free Speech and an Open Internet Values. CEAS 2004.

[25] D. Fallows. Internet Users and Spam: What the Attitudes and Behaviour of Internet Users Can Tell Us about Fighting Spam. Pew Internet & American Life Project. CEAS 2004.

[26] B. Gross. Multiple Email Addresses: A Socio-technical Investigation. CEAS 2004.

[27] J. Goodman. IP Address in Email Clients. CEAS 2004.

[28] B. Watson. Beyond Identity: Addressing Problems that Persists in an Electronic Mail System with Reliable Sender Identification. CEAS 2004.

[29] The CAN-SPAM Act. Federal Trade Commission, 2003.

[30] Pitney Bowes Study Reveals Increased Use of Electronic Communications Tools Among North American and European Workers. Pitney Bowes press release, 2000.

[31] P. Graham. A Plan for Spam. 2002. www.paulgraham.com/spam.html.

[32] P. Hoffman and D. Crocker. Unsolicited Bulk Email: Mechanisms for Control. Internet Mail Consortium Report: UBE-SOL, IMCR-008, revised May 4, 1998.

[33] Anna Ossipova. Russian State Duma to fight SPAM. 2004. http://english.pravda.ru/printed.html?news_id=13195.

[34] R. Bergman, M. Griss, and C. Staelin. A Personal Email Assistant. Hewlett-Packard Labs Technical Report, pp. 1 -23, 2002.

[35] V. P. Prakash. Vipul's Razor – A Distributed, Collaborative, Spam Detection and Filtering Network. http://razor.sourceforge.net/. Accessed: July 15, 2005.

[36] B. Gates. Buy Stamps to Send Email. 2004 http://www.cnn.com/2004/TECH/internet/03/05/spam.charge.ap/. Accessed: July 15, 2005.

[37] A. Back. Hashcash. 1997. www.hashcash.org. Accessed: July 15, 2005.

[38] N. Yvan. JMail. 2003. http://javamailclient.sourceforge.net/html_en/. Accessed: July 15, 2005.