



UNIVERSITY OF AMSTERDAM

MSc SYSTEM AND NETWORK ENGINEERING

RESEARCH PROJECT 2

Extremely Sensitive Communication

secure, secret, and private e-mail

Author:

Loek SANGERS

loek.sangers@os3.nl

Supervisor:

Ruud VERBIJ

verbij.ruud@kpmg.nl

July 4, 2016

Abstract

The focus of this research is to improve current e-mail systems to support secure, secret, and private e-mail communication. Research into this is important as with digitalizing the world, it is becoming more and more easy to conduct surveillance on a massive scale. This surveillance can put a stop to the evolution of society when people that think differently are not able to express themselves. In this research the three mentioned aspects are investigated separately in terms of what is required to achieve it, what is currently available, and what needs to be done to make the system work. Next to this, a system design is described and a list of necessary components that do not fall within the scope of this research, is given. Lastly, the feasibility of implementing this design is investigated and several use cases are described. It was found that secure, secret, and private e-mail is possible. Broad adoption is, however, preferred as this strengthens the private aspect. For this broad adoption several components will still need to be developed or finished.

Contents

1	Introduction	4
2	Literary Framework	6
2.1	SMTP	6
2.2	Secure	6
2.2.1	OpenPGP	6
2.2.2	S/MIME	7
2.2.3	opmsg	7
2.3	Secret	8
2.3.1	I2P-Bote	8
2.3.2	OnionMail	8
2.3.3	Webmail	8
2.4	Private	9
2.4.1	Mixmaster	9
2.4.2	Mixminion	9
3	Methodology	10
4	Requirements	11
4.1	Secure	11
4.2	Secret	11
4.3	Private	12
5	Available systems	14
5.1	Secure	14
5.2	Secret	15
5.3	Private	15
6	Solutions	18
6.1	Secure	18
6.2	Secret	18
6.3	Private	19
6.3.1	Spam	21

7	System	22
7.1	Sender	22
7.2	Server	23
7.3	Receiver	24
8	Feasibility	25
8.1	Secure	25
8.2	Secret	25
8.3	Private	25
8.4	General	25
9	Use Cases	27
9.1	Companies	27
9.2	E-mail providers	28
9.3	Individuals	28
10	Conclusion	30
10.1	Secure	30
10.2	Secret	30
10.3	Private	31
10.4	General	31
11	Future Work	33
	References	35

1. Introduction

It is reported more and more often that states and intelligence agencies are applying mass surveillance on the Internet [25]. In order to protect themselves against prying eyes, many people are using Virtual Private Networks (VPNs) [18]. The problem that exists with VPNs, is that they can be compelled to disclose logs by courts. If the VPN provider does not keep these logs, this protects users for partly against surveillance when browsing the internet.

In case people want to circumvent the surveillance while using e-mail, a VPN only works in disconnecting the actual IP of a person and the e-mail account of that person. This is valuable, but it does not protect the e-mail itself. Encryption standards, such as OpenPGP [1] and S/MIME [17], exist to protect e-mail, but by default the headers are not encrypted. This leaves a lot of metadata available for surveillance. It is for example known which accounts are the sender and receiver, when the e-mail is sent, and what its subject is.

In practice this metadata is protected by Transport Layer Security (TLS) between mail servers. However, even between two mail servers that support TLS it is possible to disable it dropping the StartTLS request on the network level. This is something Internet Service Providers (ISPs), and e.g. intelligence agencies, can do. This means that it cannot be assumed that e-mail is protected by TLS [7]. The question that comes to mind: how is e-mail protected?

Protection of normal e-mail from ISPs and intelligence agencies is preferred, but not necessary. However, when extremely sensitive communication is concerned this is no longer true. For the purpose of this research extremely sensitive communication is defined as any and all forms of communication that under no circumstance should be read by anyone except the sender or receiver. If such communication gets compromised this will have big consequences for the involved parties. A good example of this, is the case where it is used to report on human rights abuse, or to oppose certain regimes.

When communication is extremely sensitive there are certain aspects that should stay secret. Some of these aspects are: content, sender, receiver, duration, location, and subject. In order to keep this information secret, other data might also need to be kept secret, because this data can be used to deduce these aspects.

In order to send extremely sensitive information, no party should have

to be trusted except the receiver and sender. However, when normal e-mail is involved, multiple other parties need to be added to the chain of trust, e.g. e-mail providers and ISPs. These parties will have to abide by local law, and can possibly be influenced by powerful entities, such as intelligence agencies.

The purpose of this research is to design a system that allows users to send e-mail in a trusted way. To make sure the service can be trusted, at least the following should be arranged: data that is intercepted should not leak any information; no e-mail servers have knowledge of the content of e-mails; they actively remove metadata; and they do not keep any logs.

To address the described problem, the following research question was formulated: *How can e-mail communication be changed to provide a trusted (secure, secret, and private) way of communication?*

To be able to answer the main question on both a theoretical and a practical level, the following subquestions will be investigated:

1. What are the requirements for secure, secret, and private e-mail?
2. What are the gaps in currently available solutions with regard to these requirements?
3. What system architecture enhancements can be provided to these solutions to fill these gaps?
4. What is the feasibility of implementing these system architecture enhancements?

The focus of this research will be to investigate e-mail, other forms of communication are excluded. In order to investigate e-mail the existing protocols will be used, in favor of defining a new protocol. The goal of this research is to enable secure, secret, and private e-mail communication between users.

The main purpose of this research is to design the server side of secure e-mail communication. For users, normal e-mail clients that can send e-mails through the designed service will be supported, as well as a specialized client that can submit e-mail in a hidden way. This design is specifically created to solve issues with current implementations.

The remainder of this paper is structured as follows. First related work, both academic and created implementations, will be described. Next, the methodology is given, followed by the requirements for trusted e-mail communication. After this currently existing solutions are compared to the requirements, and other solutions are given for the found mismatches. Then, the proposed system is described in detail. Afterwards, the feasibility of this design is tested, followed by a description of possible use cases. Lastly, the conclusions and future work are given.

2. Literary Framework

Secure, secret, and private e-mail communication has been the subject of academic research for a long time. In the following subsections first Simple Mail Transfer Protocol (SMTP) will be explained followed by the three aspects as defined in the research question: Secure, Secret, and Private. For each of these three aspects existing solutions will be explained, next to this, disadvantages of the solutions will be given. A more detailed definition of the aspects will be given in section 4.

2.1 SMTP

Simple Mail Transfer Protocol (SMTP) [9] is the protocol used to exchange e-mail messages between servers. It can also be used for e-mail submission by users to their mail provider, but is not often used for e-mail retrieval. At first, SMTP was not designed with security in mind and all data traveled over the internet in plain text. The solution, as it is used now, is an encrypted TLS tunnel between servers.

For legacy reasons using this tunnel is not mandatory, but can be agreed upon between servers. This means that two parties first start a plain text connection and then ask whether TLS can be used, this request (StartTLS) is send in plain text. If the receiving server does not support TLS, the request will be ignored, and the sending server will continue just using the plain text connection. This means that any entity in control of the network can recognize the StartTLS request, and drop this request.

2.2 Secure

For the purpose of this research the secure part of e-mail is the encryption layer. Several existing methods of encrypting e-mail messages will be given here.

2.2.1 OpenPGP

OpenPGP [1] is an encryption standard that is actively being used to create end-to-end encrypted e-mail messages. The standard only provides encryption of the body of an e-mail message. This means that all headers, which include sender, receiver, and subject, are send in plain text.

OpenPGP makes use of the Web of Trust, which means that entities verify each others keys. This verification works similar to this: you trust Bob, and Bob tells you Alice is really Alice, then you know Alice is Alice. This is a Web containing you, Alice, and Bob. For the web of trust to work it is important many people are interconnected, but in practice this proves to be difficult.

There are several issues with using OpenPGP as described in [19]. The main issue is that OpenPGP does not support Perfect Forward Secrecy (PFS). This has the consequence that e-mail messages can just be stored or intercepted, and once the key gets compromised at a later time, all stored and intercepted messages can be decrypted.

2.2.2 S/MIME

S/MIME [17] is similar to OpenPGP; it also encrypts the content of e-mail messages. More specifically it encrypts and/or signs MIME type messages. S/MIME can provide authentication, non-repudiation, message integrity, and data security.

S/MIME using Certificate Authorities (CA) instead of the Web of Trust. With Certificate Authorities, you do not trust a different person to verify the identity of an individual, instead you trust the organization (CA) the user registered at.

From a companies perspective CAs are more maintainable and reliable than the Web of Trust will ever be. It does, however, come with the disadvantage that an external CA costs money, where the Web of Trust is free. On the other hand, for individuals the Web of Trust might work better, as private islands of trust can be created. This can be a more reliable form of trust on a smaller scale.

2.2.3 opmsg

Opmsg [16] is a replacement for OpenPGP [1]. It is client side software that can be used to encrypt e-mail messages. These messages can then be send using the normal SMTP protocol. Opmsg also has a way to limit the amount of metadata that is exposed. This is achieved by allowing e-mail to be send to a random mailbox at the destination provider, who in return can do the final routing to the recipient mailbox. It is even possible that the provider offers it as one single blob containing all messages for everyone. This is possible because the op-messages are self contained and ASCII-armored, which means that people can identify messages addressed to them from a group of messages.

The disadvantage of opmsg is that even though it allows for metadata obfuscation through the fact that mail providers could group all the op-messages and post them to a public webpage. This would allow anyone to visit the webpage and see the encrypted messages, but only the owner of the private key would be able to decrypt and recognize the message. Opmsg does not support a way of disallowing metadata to be gathered. This is

caused by their main advantage, it does not require any mail agent/client/daemon to be changed to use it, i.e. it can be used on top of these, which means that in transit normal SMTP will be used.

2.3 Secret

Secret e-mail is, for the purpose of this research, related to e-mail submission and retrieval. For secret e-mail this needs to happen in a hidden or covert manner.

2.3.1 I2P-Bote

I2P-Bote [8] is a e-mail system that uses the peer-to-peer I2P overlay network. It is designed to protect the privacy of its users. This is achieved by using end-to-end encryption and allowing mail relays with variable delays. As I2P is a peer-to-peer overlay network, for I2P-Bote this means that there is no centralized entity that is able to correlate enough data to determine which parties are talking to each other. [24]

The main disadvantage of I2P-Bote is the need to use an overlay network, instead of the normally used network. This means that it will only be very effective if everyone starts using this overlay network. Another disadvantage is that it does not work in combination with existing e-mail services, which might slow down adoption by the general public.

2.3.2 OnionMail

OnionMail [15] uses the Tor [21] network in combination with SMTP servers, both inside and outside the tor network, to provide secret e-mail. The effect is that the IP address of the sender is hidden from the receiver. On top of this OnionMail also removes unnecessary header information.

However, OnionMail is not very well documented and it is not stated how this protection is achieved. OnionMail requires its users to connect to it via Tor, which is a disadvantage as long as not everyone is using Tor. At the moment the usage of Tor has a bad name, and people can be identified using Tor when they are the only one doing so on the network. [22]

2.3.3 Webmail

Many of the major e-mail providers offer a webmail interface, where the client can connect using a HTTPS connection to the server. This has the result that there is no SMTP traffic to and from the end user, just "normal" web browsing traffic.

The disadvantage of most current webmail implementations for secret e-mail submission and retrieval is that often the only purpose of the server is allowing e-mail related transactions. This means that even though the traffic itself cannot be recognized as e-mail traffic, the connection can be identified as transporting e-mail traffic.

2.4 Private

During this research private e-mail is defined as e-mail that is anonymous to everyone other than the sender and receiver. A lot of research has already been conducted in the field of anonymizing e-mail, from theoretical ways using mixes [2] up to different implementations, such as Mixmaster and Mixminion.

2.4.1 Mixmaster

Mixmaster [11] is both the name of the type II remailer protocol and the most popular implementation of this protocol. The remailer protocols are described in RFCs and give a design for anonymous remailer systems. These systems aim to provide a method of sending e-mail anonymously or pseudonymously.

This is achieved by splitting the content of a e-mail message into pieces, and send these independent from each other through the Mixmaster remailer network. It is required that each piece ends at the same final remailer where it message can be reassembled and send to the intended recipient. Each of the pieces is encrypted so that every remailer on its path can decrypt only enough information to send it to the next remailer [13].

Disadvantages of Mixmaster are that it is very difficult to set up, it is not possible to reply to e-mail, and there is a high chance that during transport the e-mail gets lost somewhere [14].

2.4.2 Mixminion

Mixminion [12] is a message based remailer protocol. It builds on the Mixmaster protocol and has solved several of the issues given above. The Mixminion design provides forward anonymity by using TLS [3].

The Mixminion protocol does not use SMTP in between servers, which makes implementation on top of the existing infrastructure difficult. Another issue is that currently the network is too small to be able to be used and the project is not actively being developed since 2013 [12] [14].

3. Methodology

For the first two subquestions a literary study has been conducted. In order to answer the first question, definitions were formulated based on literature for secure, secret and private as used in the question. Next, these concepts were related to e-mail.

In order to answer the second question of this research, several implementations for secure, secret, and private e-mail have been compared. The compared system were also tested to the defined requirements. All gaps that exist between the current implementations and the needed requirements were documented.

Thirdly, solutions for the found gaps were designed. The system architecture enhancements proposed by the solutions is mostly based on previous research, but some new solutions were defined. All the enhancements together are included in a new system design.

Next, an overview of the proposed design is given. After this the theoretical feasibility of implementing the proposed design was determined. Lastly, some use cases for the proposed system were defined and described. This was done by looking at the major parties involved in sending e-mail messages, and determining what normal use cases are for these parties.

Combining the answers of the sub-research questions lead to an answer of the main research question.

Below in table 3.1 a quick overview is given:

Table 3.1: Overview of methodology

Research Question	Methodology	Expected result	Chapter
1	literary research	requirements for the three aspects description of existing systems and	4
2	literary research	their disadvantages	5
3	combining results	solution to the disadvantages	6
4	combining results	feasibility of implementing the system	8

4. Requirements

In this section the first subquestion will be investigated: *What are the requirements for secure, secret, and private e-mail?* This will be done by looking at the three aspects separately. For each of these a definition will be given, followed by what is theoretically required in e-mail to guarantee it.

4.1 Secure

Secure is a very broad term and it is even used to encompass all three aspects mentioned in this section. For the purpose of this research, e-mail will be considered secure when both the content and the subject of messages are protected even when assuming all traffic is monitored and not all servers can be trusted.

To protect the content and the subject of e-mail messages encryption can be used. The encryption needs to be end-to-end, this means that any sender is able to encrypt a message, but only the receiver can decrypt it. This can be achieved by using asymmetric encryption in combination with public and private keys.

Another preferred characteristic of the chosen encryption should be Perfect Forward Secrecy (PFS). PFS means that the message is encrypted in such a manner that it cannot be decrypted by an adversary even if the private keys of the sender and receiver get compromised at a later time.

4.2 Secret

For the purpose of this research, secret is defined as hidden from observers. More specifically it is hidden that an e-mail message is submitted to or retrieved from a mail server by a specific user. While the e-mail message is within the system it is not secret, as here only servers communicate with each other, therefore the sender and receiver are not present. Instead, during that phase, the message must be both secure and private. The aspects of e-mail submission and retrieval that can be hidden are the purpose of the traffic and both the origin and destination of the traffic.

It should be noted that in the case the mail server is compromised, the secrecy is broken by default. This is because the submission is a shared

secret of the sender and the mail server, and the retrieval is a shared secret of the mail server and the recipient.

The purpose of secret e-mail is to allow people that are under surveillance to send and receive e-mail messages, without this being known to the surveilling party. This means that the secret aspect is not needed for every user of the system, but only for those that require an extra layer of security. Other users could just use both the secure and private aspect in order to hide the content of their conversation as well as the parties involved in the conversation, but not the fact that they are having a conversation.

SMTP does not allow for this, as messages are submitted and retrieved using the normal internet with known protocol that are only used for this purpose. This means that either the protocol has to be circumvented or the fact that the protocol is used has to be hidden, to hide the purpose, and that an anonymizing overlay network should be used to hide the origin and destination of the traffic.

Circumvention of the protocol can be achieved by accepting a different and hidable method of submission to the server. This can be done by for example making it look like a normal HTTPS over TLS connection. If the data transmission from client to server and back is similar to normal HTTPS traffic, it can not be deduced e-mail was submitted or retrieved over this connection.

Hiding that SMTP is used by a specific user, could be achieved by using overlay networks, such as Tor and I2P. This does not hide the fact that there is mail traffic between the mail server and the overlay network, but the end user is identifiable as being the origin of the e-mail message - this needs to be guaranteed by the overlay network. This means that mail traffic cannot realistically be linked to the actual sender or receiver.

Another way of hiding that SMTP is used by a specific user, is routing traffic through a VPN tunnel to the e-mail server. When doing this, it is important to use this VPN connection for both e-mail related traffic and other internet traffic. Otherwise the presence of the VPN connection itself implies e-mail is being sent or received.

4.3 Private

For the purpose of this research private is defined as the only entities that know both the sender and the receiver of an e-mail message are exactly these two entities. This means that it is still considered private when the mail server that the sender or receiver directly communicates with, knows a message was sent or received by that specific user. All other servers must not be able to know or deduct who the sender and/or receiver are, but they may know which servers are exchanging messages.

To guarantee privacy both the sender and the receiver need to be able to verify the identity of each other. This can be achieved by using signatures.

This combined means that e-mail messages are private and anonymous while in transit, but while in the hands of the sender or the receiver the messages are not anonymous anymore.

As an e-mail message in transit must be private all metadata that could be used to break the privacy, needs to be removed. For this research the following meta information is considered to break privacy:

- Information directly connected to sender or receiver
 - IP address
 - E-mail address
 - Signature or certificate
- relation between incoming and outgoing messages on servers
 - content
 - timing
 - ratio

A problem that is created with private e-mail is that spam detection by servers becomes more difficult. When the service truly anonymizes the e-mail messages, any malicious entity could use the system to send spam messages. The proposed mail service should gracefully stop spam in a reliable manner, in order to not get the service blacklisted by other parties.

5. Available systems

In the previous section the requirements for secure, secret, and private e-mail communication are given. Current implementations, such as the ones given in section 2, do not implement all of these requirements. In this section the currently available systems will be compared to the requirements and all gaps found will be documented.

5.1 Secure

As mentioned in section 4.1 both end-to-end encryption and Perfect Forward Secrecy (PFS) are needed for secure e-mail. There are two main methods in use today that provide end-to-end encryption of the content of an e-mail message: OpenPGP and S/MIME [23]. However, both these methods do not provide PFS.

For PFS only opmsg, as described in section 2.2.3, was found to provide it for e-mail messages. Opmsg has not become popular as of yet, and the user base is therefore quite small.

In practice the current state of encryption is up to the task of securing e-mail messages, it just has to be implemented correctly. The main issue with end-to-end encryption and PFS is the need for a scalable Key Distribution System (KDS) that anyone can use anonymously.

For PFS there are workarounds for the required KDS, e.g. sending the next keys needed to reply to a message signed and encrypted in the previous message. The initial problem of exchanging keys, however, still stands.

Another issue with providing end-to-end encryption and PFS is that non-technical users need to be able to easily use it. This means that the key management, which is required for both end-to-end encryption and PFS, needs to happen without the user having to worry about it.

When users use a dedicated e-mail client this is not really a problem as the key can then be stored on disk and the software can be verified. For webmail this is, however, not possible. A solution for webmail would be to use a plug-in that handles the keys and the encryption, both Google and Yahoo are currently developing a plug-in like this [6].

In summary, the major gap in providing secure e-mail is the lack of a scalable KDS in combination with the lack of available and easy to use client software.

5.2 Secret

For secret e-mail the submission and retrieval of messages has to be hidden from an observer, as mentioned in section 4.2. Two methods to achieve secret e-mail submission and retrieval are: Circumventing use of SMTP and hiding that a specific user is using SMTP.

An example of circumventing the SMTP protocol, as described in section 4.2, is by using an HTTPS connection. For this to work properly and really hide the e-mail traffic, normal HTTPS traffic with similar characteristics needs to be present as well.

The main issue with this, or similar solutions, is that the end point can be put under surveillance. This means that all traffic to and from this (mail) server will be made suspicious. In extreme cases the server can also be forced, e.g. via court orders, to disclose which connections were e-mail related and which were not.

Hiding that a specific user is using SMTP, can be achieved by using a anonymizing overlay network, as described in section 4.2. Using these networks only really anonymizes the users, when enough people use it.

This is caused by the fact that the anonymizing factor is that traffic is bounced around between many users, in order to mask which user is doing what. If not many users are present, this might be breakable by someone being able to monitor enough of the network.

In summary, hiding the purpose and origin of traffic is what is required for secret e-mail. The two main ways of doing this is using an encrypted connection to hide the purpose and using an anonymizing overlay network to hide the origin. For both of these many implementations exist, such as VPN solutions and Tor respectively.

5.3 Private

For an e-mail message to be private, as defined in section 4.3, only the sender and receiver of the message should be aware of who the other is. In order to achieve this, metadata that breaks this privacy needs to be removed. The following metadata has been identified: Information directly connected to sender or receiver, such as IP and e-mail address; and relation between incoming and outgoing messages on servers, such as content, timing, and ratio.

A lot of research has already been performed on how to anonymize e-mail messages using remailers, such as Mixmaster and Mixminion. Both these remailers describe how the metadata can be removed in order to fully anonymize messages. The purpose of this research is not to create fully anonymous e-mail, but to make it so only the sender and receiver are aware of the other. However, it is more feasible to create fully anonymous e-mail and then sign the message before all encryption steps. By signing before the encryption takes place, the signature will only be visible to the recipient once he has decrypted the e-mail message, so the identity of the sender is still hidden.

There are several issues that exist for both remailers. A more detailed look at the issues of Mixmaster, as described in [5], is given below:

Client knowledge of available servers For Mixminion to work, e-mail messages are sent from one server to another server. The client decided the order in which the servers are traversed in combination with which servers are used. This means that if an adversary can make sure only a certain user knows about a server, and this server is used, the adversary can conclude the user is sending an e-mail message.

More extended information can also be gathered by for example making sure the client only knows compromised servers. The entire path of any e-mail message can then be tracked breaking the privacy of the conversation.

Subpoena attack In essence the subpoena attack works by either passively or actively gathering possibly encrypted e-mail messages. At a later time the service provider can be compelled by a subpoena to provide relation between incoming and outgoing e-mail messages. An example of how this could work is, when a government agency is surveilling a specific person, and sees an e-mail message is sent in an encrypted manner, this message can be copied. Then after it reaches the first server, all outgoing messages in combination with their destination can be recorded.

For this method to work, the surveilling entity will have to be able to record all messages within the network that is used by the two people sending messages. In practice this network can change for different messages from the same people, therefore the surveilling entity needs to basically record all messages that are being sent, which is difficult only when the network is big enough.

Once the messages are gathered, the e-mail service providers can be compelled to recalculate the relation between the ingoing and the outgoing message under investigation. The difficulty of obtaining the subpoena is different for different legislations, but it is a possible attack vector on the existing system.

Expiration date partitioning In order to protect against e-mail messages being replayed by an adversary, Mixmaster added a date to the message format. This date is not the exact date of sending, but within a range of three days before or after the sending time.

This, however, opens for an attack where an adversary delays certain e-mail messages for some time. This time should not be too long as then the messages get discarded by the next server as being replayed, but the uniformity in the date of the messages is broken by delaying some messages.

This means that for example all of the messages except target messages get delayed by a malicious server. When the messages pass a normal server nothing special happens, but if the messages after a normal server end up at a malicious server again with a future time, it can be deducted that these are either new messages from the normal server, or the targeted messages.

This attack requires adversaries to be in control of multiple servers, so the likelihood is not very high. The impact of the attack is, however, rather high as it can be used to de-anonymize people.

Tagging attack Tagging attacks can be used to identify e-mail messages over multiple servers, and decryption steps. The attack can happen on either the headers, or the payload in Mixmaster. All headers contain a hash, but this only encompasses the content of that specific header itself. This means that some bits can be flipped in a later header, and if this happens to be the header corresponding to a malicious server, the message can be recognized and identified.

Another possibility is to tag the payload by flipping some bits there. As the hash does not contain any information on the payload, it can not protect against this form of attack. Malicious servers can then try to identify the changed payload and link it to the corresponding message, again to de-anonymize people.

The four attacks described here have been solved in Mixminion as described in [5]. For both the subpoena attack, and the expiration date attack a solution is to have a frequent key rollover, in combination with removing the date altogether. This means that the server will be unable to interpret an old message after a key rollover has taken place.

The tagging attacks can be resolved by making the hash include all headers and the payload. This has the result that if a tag is placed the hash will be incorrect, and the message can therefore be marked as insecure.

Solving the client knowledge attack is more difficult as it requires a way that client can be sure they have the same knowledge as other clients have. In order to achieve this, some form of directory server system needs to exist that can guarantee clients have the same view of the network. This system will also have to be distributed so an adversary cannot just abuse this system to execute the client knowledge attack.

These solutions could also be implemented on top of SMTP, as these have nothing to do with the way e-mail is transported between servers. The advantage of running the system on top of SMTP is that currently SMTP is the major, or even only, protocol used for e-mail transmission.

Another issue, as stated in section 4.3, is spam. The current solutions, Mixmaster and Mixminion, resolve this by allowing recipients to opt-out of receiving e-mail messages from the service. While this works as a deterrent for spam senders to use the service, it would not work when the system is the most used way for sending e-mail.

6. Solutions

In this section possible solutions for the issues found in section 5 will be given in order to answer the third research question question: *What system architecture enhancements can be provided to these solutions to fill these gaps?*. This will again be done by addressing the three aspects of trusted e-mail in the respective order: Secure, Secret, and Private.

6.1 Secure

There are no real gaps between requirements and available solutions in terms of secure e-mail. The only real issues for it are the Key Distribution System (KDS) and lack of available easy to use client software, as described in section 5.1.

Both these issues fall outside of the scope of this research. It should, however, be noted that both Google and Yahoo are working on both issues in order to provide secure end-to-end encrypted e-mail.

The Perfect Forward Secrecy (PFS) is not included in this, but once the KDS is in place, it should be trivial to support a form of PFS, e.g. as done by opmsg.

In order for these issues to be solved it is important that people, as in (potential) customers, want the security features for their e-mail messages. When this is the case, solving the issues will become a market opportunity and advertisement material. Which makes implementing the features a profitable investment for the companies that provide e-mail services.

It should be noted that to support activists or other people that need a secure way of communication, public adoption is not mandatory. The system will work as well without the scalable KDS. Users will just have to exchange keys out of band, which might even be preferable for people under surveillance if a scalable KDS did exist.

6.2 Secret

For secret e-mail to be possible, it has to be hidden that a specific user is sending e-mail messages. To a smaller extend it can also be hidden by circumventing the SMTP protocol and using for example HTTPS.

This solution is, however, not perfect, because in the end the mail server will always know which entity connected to it to send e-mail as anonymous e-mail is not just accepted. The identity of the entity is not only the account name that send the e-mail, but also the connected IP-address. This means that under legal pressure, this information might need to be revealed. Even though servers can decide not to gather and store this information, the end user will have to fully trust the provider on this.

In case the server is not aware which IP-address is actually in control of the connection, only the account could be given under legal pressure. This means that for truly secret e-mail an overlay network that really anonymizes its users needs to be used. This network also needs to support multiple use cases next to e-mail, to not give away information based on being connected to the network.

At this moment, networks like this exist, e.g. Tor. These networks are, however, not used everywhere, which decreases their anonymizing potential. Furthermore, Tor has a bad name, and this will need to somehow be changed for it to gain a big user base.

Everything needed for truly secret e-mail exists, e.g. webmail on a server with multiple purposes via an anonymizing overlay network. It is, however, not possible to actively use it without drawing suspicion, as the use of anonymizing overlay networks themselves put people under investigation and suspicion. For this to change, public opinion will have to support anonymizing networks, despite the fact that these can be used for criminal activities.

6.3 Private

As mentioned before, a lot of research has been done in the field of anonymous e-mail. The solutions found for this can be directly used, as well as improvements on these solutions. The basis of most of the solutions are mixes as first introduced in [2]. There are several ways these mixes can be used to hide the relation between incoming and outgoing messages. The main ways that are implemented for e-mail anonymizing systems are described in [20].

The distinction is made between simple mixes and pool mixes. The first is either a threshold mix, which forwards its messages after receiving more than the set threshold, or a timed mix, which forwards its messages every x amount of time. Pool mixes add a pool to these option, this means that all messages that come in enter the pool and at the moment the server forwards its messages a random selection of messages in the pool is send depending on a threshold and/or time as well.

There are some newer mix designs that improve the anonymity provided as described in [10]: Multi-Binomial Shared-Pool Mix (MBSP Mix) and Multi-Binomial Independent-Pool Mix (MBIP Mix). Both of these methods are binomial mixes, which work as follows: All incoming messages are placed in a message pool, from this pool messages are selected by a binomial function. This function can be seen as flipping a biased coin for

each message, and this coin flip decides whether the message stays in the pool or is moved to the outgoing pool. The bias depend on the binomial function.

For MBSP Mix all messages are still placed in one incoming pool, but there are multiple binomial functions to decide the bias of the coin flip. For every batch one of the functions is selected at random, and applied. The main advantage of this, is that the correlation between incoming and outgoing messages, can not be predicted, as it is not know which binomial function was chosen, and what the dependencies of this function are.

For MBIP Mix there are multiple pools for incoming messages instead and each pool has one dedicated binomial function to decide the bias of the coin flip. The messages are divided over the different pools in a manner unknown to an external adversary. The fact that each pool has its own bias function, has the advantage every channel can have a different delay.

For the purpose of an e-mail forwarding mix, it should not be possible to indicate which type of delay is preferred. Instead the mix should pick a pool at random for each incoming message, this means that the difference in latency is not utilized to achieve a multiple purpose mix, but to decrease the predictability of the relation between incoming and outgoing messages.

Both MBSP Mix and MBIP Mix anonymize messages to a greater extend than previously designed systems. If a new better mix algorithm would be designed, it is also easy to integrate it into both of these designs, as they are already build on combining existing solutions to obfuscate relations between incoming and outgoing messages.

The existing attacks on mix systems mostly depend on either being able to predict relations or on being able to empty pool of legitimate messages. Both these aspects are more difficult to perform against MBSP Mix and MBIP Mix. Therefore new attacks will have to be developed, or existing attacks will have to be adapted.

Another aspect for known attacks is the number of users in relation to the number of messages in the system, and more specifically in a pool on the mail server. The strength of the network is highly dependent on this relation, the more possible users per message the better the system will work.

To achieve privacy, on top of the proposed anonymous e-mail service the message needs to be signed. In subsection 6.3.1 more details will be given about where signatures are needed, and of what kind in order to also be to counter spam as well as achieve privacy.

The main issues with achieving privacy as described in this section are: the lack of a directory server system that makes sure a users have the same view of the topology of the network and the lack of many users in its early stages.

Of these the first is a technological difficulty, and the second is a public opinion issue. This makes it that in practice the second issue will either solve itself, or be near impossible to change. Both are outside of the scope of this research.

6.3.1 Spam

To solve the issue of malicious users abusing the e-mail service for spam several measures can be taken. None of these is perfect in preventing spam, but all of them make the process more time consuming and less reusable.

First of all, profiling can be done on the sender by the submission server. If the behavior all of a sudden changes, this can be used as indication and for example rate limiting can be applied.

Another measure is to do filtering on the last mail server. All e-mail messages send through the proposed service, will have a specific format, containing random ASCII characters. In case the message contains plain-text the server can conclude something is wrong, and apply its normal spam filtering.

It is also possible to require the end-to-end encrypted message to be signed using the public key of the recipient and to mark messages send through the service with a header. This way the last server can verify the signature made with the public key of the recipient when it encounters the header. If an invalid signature is found, the server can drop the message.

On top of this the unencrypted message needs to also be signed by the sender. In the case this signature is missing, the message can also be moved to the spam folder after being decrypted by the receiver. This means that a valid private key needs to be used to send the message. When a user then sends spam messages, this user can be reported and flagged in the KDS, so when the next e-mail is submitted the identity can be rejected by the submission server.

This combined means that any spam would have to be targeted at a specific person. The message would then have to be encrypted and signed with the public key of the recipient and send through the mail service. This means that the message cannot be send to multiple recipients at once, but will have to be re-encrypted and resigned for every target recipient.

7. System

In this section the proposed system will be given. This will be done by describing how an e-mail messages traverses the system from sender to receiver. This is done to combine the solutions given in section 6 and does not answer a research question by itself.

7.1 Sender

The sender of the e-mail message has to start with writing the message. Next to this the recipient e-mail address and public key needs to be known and possibly imported from a trusted Key Distribution System (KDS).

The sender then signs the unencrypted message with his private key. This makes sure that the recipient can verify the receiver, and when this signature is missing the e-mail is more likely to be spam. The combination of the message and this signature needs to have a fixed size. if the size of messages is allowed to be different, messages in the system can be identified by their size, which breaks the private aspect of the system. Next, the message is encrypted with the public key of the recipient. This encryption should provide Perfect Forward Secrecy (PFS) and creates the end-to-end protection for the content of the message. Then the encrypted e-mail is signed with the public key of the recipient. The purpose of this signature is to enable spam filtering on the server side, which will be described in the next subsection.

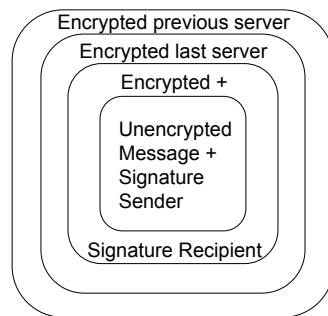


Figure 7.1: Content Encryption

The sender then picks a chain of mail servers that the message will use in order to arrive at the recipient. To be able pick these server, a complete list of the network should be retrieved in a secure and trusted way, e.g. using a directory service. The assumption is made for the purpose of this design that this is possible for the sender.

After the sender has chosen the chain of servers, the message will be encrypted for each server, and a header will be added for each step. The above described message is first encrypted for the last server and an encrypted header is added containing the information to reach the next step in the chain. This process is repeated for each consecutive server up to the first server.

Lastly, the sender submits the message to the first server of the chain.

7.2 Server

Each server along the chain decrypts the message with its private key, and forwards it to the next step in the chain. The servers make sure that there is no perceivable relation between incoming and outgoing messages. Before the message is forwarded, a new random header is added at the bottom of the header list in order to keep the number of headers constant. The header also contains a hash of the message so it can be verified the message has not been tampered with.

The relation is between incoming and outgoing messages broken by implementing either a Multi-Binomial Shared-Pool Mix (MBSP Mix) or Multi-Binomial Independent-Pool Mix (MBIP Mix) mix mail server. Both of these, when implemented correctly, make sure that it is not possible to match the incoming message with the related outgoing message.

On the last server the message will get delivered to the mail box of the recipient. In order to do this some extra steps are taken. First of all, the message is decrypted as normal. Next, the signature on the end-to-end encrypted message is verified. When the signature is correct the message is delivered to the mail box, otherwise it is dropped. This last step will stop easy abuse of this system for spam messages. Each message will have to be signed with the public key of the recipient, which makes it more resource intensive to send spam messages.

Next to forwarding legitimate e-mail messages, mail servers can also create dummy messages. These message are used to fill the network, and make it more difficult to trace any particular message. An extra implementation with these dummy messages is to make sure that the dummy message ends up at the sending server after a few hops. This can enable the server to notice it is under attack, or links are broken, if all of a sudden the dummy messages disappear. This is described in more detail as a Red-Green-Black Mix in [4].

7.3 Receiver

Once the message is received it needs to be decrypted using the private key of the recipient. When this decryption is done, the signature of the sender needs to be verified. In case this signature is missing the message should be moved to the spam folder.

In order to reply the recipient will have to create its own message with the previous sender as recipient. This is to allow for a different path of servers to be in between the sender and receiver on the return path.

8. Feasibility

In this section the fourth subquestion, *What is the feasibility of implementing these system architecture enhancements?*, will be addressed. This is done by discussing the feasibility of each of the aspects, followed by a general answer.

8.1 Secure

Both issues as described in section 6.1 can be solved by an implementation. The easy to use client software is a matter of making an easy to use user interface, which is certainly possible. Implementing the Key Distribution System (KDS) in a scalable and easy to use manner is more difficult. This is, however, a current project of both Yahoo and Google.

8.2 Secret

From a technological point of view, secret e-mail is already possible. The only shortcoming is broad user adoption of the tools needed, such as overlay networks, and offering webmail services that share network resources with other purposes that generate similar traffic. The latter can be implemented by any e-mail provider that has a webmail client by also hosting a website, such as a forum, on the same IP-address.

8.3 Private

The anonymous aspect of the private e-mail messages is the most difficult part. The server and network properties have been designed academically, but not been implemented yet. This implementation will need to be easy to deploy and adopt on top of current systems, which will make it difficult to implement.

8.4 General

All in all implementing secure, secret, and private e-mail communication software for both the server and the client is feasible, whether it will be

adopted by the public is a different matter entirely, and can not be predicted.

Furthermore, what is proposed are not so much system enhancements as components gathered from different systems to be combined into a new more sound system.

9. Use Cases

In this section several use cases for secure, secret, and private e-mail communication will be given. The use cases discussed in order are: communication between companies, and between individuals. For both of these entities with a previous relation and without any existing relation will be discussed.

9.1 Companies

In the case, two companies have an existing relation and employees exchange sensitive information via e-mail messages, these messages should be protected against eavesdropping. With existing solutions it is possible for employees to encrypt messages for the recipient, but this happens on the client side. In addition, this encryption does not extend to the subject of the message, or the participants of the conversation.

These three aspects can be achieved by letting employees submit e-mail messages to the local mail server as normal. On the mail server the messages can be encapsulated into a generic message between the two companies. The content of the generic message is the complete original message in encrypted form. This encryption is done on the server of the sender, and it is decrypted on the server of the receiver, and delivered as if the decrypted message was normally received.

As an example say employee A of company B and employee C of company D want to exchange secure e-mail. In the current system a message could be sent from A@B.org to C@D.org, but on the network layer it would be possible to see that A is communicating with C and what the subject of their e-mail message is.

It is possible to change this so both end users do and see exactly the same, but now the mail servers change the message sent between them. Company B would encrypt the message and send it as mail@B.org to mail@D.org, company D would then decrypt the message and forward it to employee C.

Providing this service to employees can be valuable to better secure company secrets. Another aspect it provides is a way of communication between two highly placed employees, e.g. CEO's, without this possibly being known to outside entities based on e-mail traffic.

In the case the companies also want to hide that they are communicating in general, the decision can be made to use the proposed mail service

between the mail servers of the companies.

The main advantage for companies is that they do not have to distribute keys or certificates to all of their employees. Instead companies only need to exchange public keys with each other in a secure and verified manner.

9.2 E-mail providers

A special case of two companies building this system, is when both are e-mail providers. In this case they can offer secure and private e-mail to its users towards the other company.

The in transit protection of the e-mail messages could be protected by TLS when the companies enforce a policy to not exchange messages if Start-TLS is not successful. The advantage of implementing the proposed system, even if only partly, is that the data at rest at intermediate servers is protected against anyone but the targeted recipient company.

Furthermore, it will allow users to set up "secure e-mail channels" by making a chain of many e-mail addresses from different providers that automatically forward messages to a next account. When the messages in transit are guaranteed to be protected, this would result in a multiple court orders to get to the next step in the channel. When while setting this channel up, different legislative areas are chosen, doing this can be a cumbersome activity, at will make it way more expensive time wise to follow the trail. It should be noted, that this is most likely only true for the first use of the channel, because once it has been figured out, the next use of the channel can be assumed to lead to the same target.

Next to this, if e-mail providers decide to partly implement this, it will be easier to build on top of this and make "virtual" mail servers that as connection to the internet only have one or more e-mail addresses, and performs the decryption and forwarding steps with the messages it receives.

This method will also make it more difficult to take down the system, as it is hidden behind an e-mail address that can easily be replaced. The real server will have to retrieve the messages send to its e-mail addresses somehow, but this could be done via anonymizing overlay networks to obfuscate the link to the server.

9.3 Individuals

There are many cases where individuals would want to communicate, while being sure noone else could listen in to the conversation. The main examples used are either criminals or political dissidents. This means that there is an ethical debate here in whether a completely private form of communication is even wanted.

To fully address this ethical debate, different study would have to be conducted with this as main purpose. The main sides are that for the political landscape to evolve in any way, new ideas need to be able to be freely exchanged with like minded individuals.

For criminal the designed system will, of course, be beneficial. This does not mean that anything is standing in the way of said criminal to create such a system themselves and thereby protecting them against eavesdropping by state agencies or different entities.

Different use cases for communication between individuals could also be more innocent like a normal conversation between people that are aware of their privacy and want to be sure to stay private. This could range anywhere from between family to between state leaders.

All in all, it is important governments make a decision in whether to support private communication or oppose it. This decision should be defended towards their population and in the case the majority people disagree, during a future election a party can be chosen that moves in the other direction.

10. Conclusion

To be able to answer the research question, first all three aspects, secure, secret, and private, will be summarized in short. After this the aspects will be combined in an answer to the general question.

10.1 Secure

Secure e-mail is defined as e-mail for which both the content and the subject is guaranteed to be unable to be understood even when the message is seen by an adversary while in transit. This can be achieved by providing end-to-end encryption, for more protection the encryption should also be provided with Perfect Forward Secrecy (PFS).

Currently there are systems, e.g. opmsg, that provide end-to-end encryption with PFS. The main standing issues with providing this, is that there is no easy to use Key Distribution System (KDS) freely available. The systems that exist now, such as Certificate Authorities, could fill this role, but are not easy to use and free. Research is also being conducted to create a new type of KDS that is both easy to use and cheaply available.

This means that implementing secure e-mail communication is mainly a matter of creating an easy to use client, or browser plugin for webmail, that handles the technical aspects, and either using an existing KDS or waiting for a newly designed version.

10.2 Secret

Secret e-mail is achieved by providing a way to submit and retrieve e-mail from mail servers in a hidden and covert manner. This means that an observer will be unable to know with certainty that a person has either send or retrieved e-mail.

This secrecy is not included in the existing Simple Mail Transfer Protocol (SMTP), and therefore it will have to be provided using a different protocol. In theory any encrypted channel, such as a TLS or VPN connection, to the mail server that has a different purpose will suffice to provide secrecy at least partly.

On top of this an anonymizing network, such as Tor and I2P, can provide even more anonymity. However, this is only the case when many people use

these networks. If very little people use them it works counter productive, as users will stand out instead of be hidden.

Providing secret e-mail is possible right now, as the anonymizing networks exist and giving a server multiple purposes is also possible. To become fully operational many more people will have to start using an anonymizing overlay network and mail providers will need to have an incentive to give multiple different purposes to their mail servers.

10.3 Private

E-mail is private when the only parties that are aware who both the sender and the receiver are, are exactly the sender and the receiver. This means that while in transit the e-mail is anonymous, but once it has arrived the identity of the sender can be verified.

The available systems use mixes in order to anonymize the e-mail and some of the proposed mix systems, such as Multi-Binomial Shared-Pool Mix (MBSP Mix) and Multi-Binomial Independent-Pool Mix (MBIP Mix), suffice for the purpose of anonymous e-mail. The main unsolved issue is to design a way that both servers and clients can gain knowledge of what servers are part of the mix network. This system needs to be designed in such a way that an adversary cannot force people to only use certain server that they control, instead of all servers.

Several solutions to filter spam have been found. The main principal to reduce spam is that all messages that are not encrypted and signed with the public key of the recipient, should not be delivered to the mail address of that recipient. This means that a single spam message cannot be send to multiple people using the system, but the message will have to be encrypted and signed for each individual e-mail address.

The feasibility of implementing private e-mail is debatable. On a technological level only the directory service for the mix network is really needed, but on a practical level many mail servers will have to start running different software or software extensions. This means that until either companies or a large group of people have found a reason to provide this service to many users, it will be very difficult to achieve. At the same time the new system will have to be adopted by many users, to be able to fully anonymize its users.

10.4 General

The proposed system uses several aspects of existing implementations or research to be able to provide secure, secret, and private e-mail communication.

On a technological level there are only several components left to be designed to be able to provide a secure, secret, and private method for e-mail communication. These issues are: KDS and secure directory service.

Next to this some implementation have to be created, but the theoretical background already exists.

However, on a society level a lot has to change for secure, secret, and private e-mail to become commonplace. First of all, the public has to demand this service an mass from both companies and governments. The other option is for companies or governments to want to provide it to the public for their own reasons, and make it the default without the user actually noticing. There are several use cases that could help the adoption of the proposed system, such as inter-company implementations.

11. Future Work

Future work building on this research on a practical level is to implement the needed systems: e-mail server, directory server, KDS, and client software. All of these need to be easy to use and deploy, to have a fighting chance in the real world.

Next to the practical level, there are also possibilities on an academic level. These are, however, not technical. Examples of academic research could be to investigate how the people perceives e-mail security and privacy, and find ways to better educate them. Other than this it is also valuable to look into the public opinion of people about what role companies play in this.

Lastly, research into the market value for companies to implement systems as described in this paper would be of huge value. If the outcome of a such research is that it profitable to implement the proposed systems, this could meant that companies will try to make money by implementing it, and thus convince people to use their systems because of the added value.

Acknowledgements

I would like to thank KPMG for the opportunity to do this research. It was a great to be able to define a specific project that I am personally interested in from the broad subject they offered as general basis. I would like to thank Ruud Verbij, my supervisor from KPMG, for his supervision, great advice, and his help in general during the project. I also want to thank my fellow student, Romke van Dijk, for sparring over ideas during my project as well as reviewing the paper. Furthermore, I would like to thank the SNE group and the OS3 education for providing me with a great year with this project at its end.

References

- [1] J. Callas et al. *OpenPGP Message Format*. RFC 4880 (Proposed Standard). Updated by RFC 5581. Internet Engineering Task Force, Nov. 2007. URL: <http://www.ietf.org/rfc/rfc4880.txt>.
- [2] David L Chaum. “Untraceable electronic mail, return addresses, and digital pseudonyms”. In: *Communications of the ACM* 24.2 (1981), pp. 84–90.
- [3] George Danezis, Roger Dingledine, and Nick Mathewson. “Mixminion: Design of a type III anonymous remailer protocol”. In: *Security and Privacy, 2003. Proceedings. 2003 Symposium on*. IEEE. 2003, pp. 2–15.
- [4] George Danezis and Len Sassaman. “Heartbeat Traffic to Counter (N-1) Attacks: Red-green-black Mixes”. In: *Proceedings of the 2003 ACM Workshop on Privacy in the Electronic Society*. WPES '03. Washington, DC: ACM, 2003, pp. 89–93. ISBN: 1-58113-776-1. DOI: 10.1145/1005140.1005154. URL: <http://doi.acm.org/10.1145/1005140.1005154>.
- [5] Roger Dingledine and Len Sassaman. *Attacks on Anonymity Systems: The Theory*. Blackhat.
- [6] Lorenzo Franceschi-Bicchieri. *The Dream Of Usable Email Encryption Is Still A Work In Progress*. URL: <http://motherboard.vice.com/read/google-yahoo-end-to-end-email-encryption-work-in-progress> (visited on 06/10/2016).
- [7] Jacob Hoffman-Andrews. *ISPs Removing Their Customers’ Email Encryption*. URL: <https://www.eff.org/deeplinks/2014/11/starttls-downgrade-attacks> (visited on 06/07/2016).
- [8] I2P-Bote. *I2P-Bote*. URL: <http://bote.i2p.xyz/> (visited on 06/03/2016).
- [9] J. Klensin. *Simple Mail Transfer Protocol*. RFC 5321. <http://www.rfc-editor.org/rfc/rfc5321.txt>. RFC Editor, Oct. 2008. URL: <http://www.rfc-editor.org/rfc/rfc5321.txt>.
- [10] Shaahin Madani. “Improving security and efficiency of mix-based anonymous communication systems”. In: (2015).
- [11] Mixmaster. *Mixmaster*. 2012. URL: <http://mixmaster.sourceforge.net/> (visited on 06/03/2016).

- [12] Mixminion. *Mixminion*. 2013. URL: <http://mixminion.net/> (visited on 06/02/2016).
- [13] U Moeller. *Mixmaster Protocol Version 2*. Internet-Draft draft-sassaman-mixmaster-03. <http://www.ietf.org/internet-drafts/draft-sassaman-mixmaster-03.txt>. IETF Secretariat, Dec. 2004. URL: <http://www.ietf.org/internet-drafts/draft-sassaman-mixmaster-03.txt>.
- [14] Steven J. Murdoch. *Current state of anonymous email usability*. URL: <https://www.lightbluetouchpaper.org/2014/04/03/current-state-of-anonymous-email-usability/> (visited on 06/08/2016).
- [15] OnionMail. *OnionMail*. URL: <http://en.onionmail.info/what.html> (visited on 06/03/2016).
- [16] opmsg. *opmsg*. URL: <https://github.com/stealth/opmsg> (visited on 06/03/2016).
- [17] B. Ramsdell. *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification*. RFC 3851 (Proposed Standard). Obsoleted by RFC 5751. Internet Engineering Task Force, July 2004. URL: <http://www.ietf.org/rfc/rfc3851.txt>.
- [18] Claire Reilly. *VPN use skyrockets in Australia amid privacy concerns*. URL: <http://www.cnet.com/au/news/vpn-use-increases-in-australia-amid-data-retention-and-piracy-concerns/> (visited on 06/07/2016).
- [19] secushare.org. *15 reasons not to start using PGP*. URL: <http://secushare.org/PGP> (visited on 06/16/2016).
- [20] Andrei Serjantov, Roger Dingledine, and Paul Syverson. “From a trickle to a flood: Active attacks on several mix types”. In: *International Workshop on Information Hiding*. Springer. 2002, pp. 36–52.
- [21] Tor. *Tor*. URL: <https://www.torproject.org/> (visited on 06/08/2016).
- [22] Lisa Vaas. *Use of Tor pointed FBI to Harvard University bomb hoax suspect*. URL: <https://nakedsecurity.sophos.com/2013/12/20/use-of-tor-pointed-fbi-to-harvard-university-bomb-hoax-suspect/> (visited on 06/08/2016).
- [23] Wikipedia. *Email Encryption*. URL: https://en.wikipedia.org/wiki/Email_encryption (visited on 06/10/2016).
- [24] Wikipedia. *I2P*. URL: <https://en.wikipedia.org/wiki/I2P> (visited on 06/08/2016).
- [25] Wikipedia. *Mass surveillance*. URL: https://en.wikipedia.org/wiki/Mass_surveillance (visited on 06/07/2016).