

# Comparison of the privacy facilities of Gmail with those of Hotmail

August 2010

A.P.C. Sudeera Jayasekara  
csudeeraj@gmail.com

**Introduction**

This document intends to compare and contrast the privacy measures supported by the mail providers Gmail and Hotmail.

The two mail providers were assessed according to the privacy features provided for the following list of criteria,

1. Account Creation
2. User Authentication
3. Message Authentication
4. Attachment Safety
5. Spam Handling
6. Mail data storage and mail transport

## 1. Account Creation

In order to compare the privacy involved in the account creation phase of the two email providers, the following data was extracted,

### 1.1 Gmail

Extracted from Gmail account creation page [1]

The page uses HTTPS and it uses the following security measures,

- Transport Layer Security Version 1.0 (TLS v1.0)
- 128 bit Alleged RC4 (ARC4) encryption
- Hashing Algorithm 1024 bit RSA/SHA

Field	Value
Version	V3
Serial number	2f df bc f6 ae 91 52 6d 0f 9a a...
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	Thawte SGC CA, Thawte Cons...
Valid from	18 December 2009 05:30:00 AM
Valid to	19 December 2011 05:29:59 AM
Subject	www.google.com, Google Inc,...
Public key	RSA (1024 Bits)
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Enhanced Key Usage	Server Authentication (1.3.6....
Authority Information Acc...	[1]Authority Info Access: Acc...
Basic Constraints	Subject Type=End Entity, Pat...
Thumbprint algorithm	sha1
Thumbprint	40 50 62 e5 be fd e4 af 97 e9 ...

#### Certificate summary

Holder: www.google.com, Google Inc  
 Issuer: Thawte SGC CA, Thawte Consulting (Pty) Ltd.  
 Expires: 18/12/2011 11:59:00 PM GMT  
 Encryption protocol  
 TLS v1.0 128 bit ARC4 (1024 bit RSA/SHA)

Opera 10.60

MS IE 8.0

For creating an account with Gmail, a user needs to specify a password which is having a minimum of 8 characters in length.

## 1.2 Hotmail

Extracted from Hotmail account creation page [2]

The page uses HTTPS and it uses

- Transport Layer Security Version 1.0 (TLS v1.0)
- 128 bit Alleged RC4 (ARC4) encryption
- Hashing Algorithm 1024 bit RSA/MD5

Field	Value
Version	V3
Serial number	16 a2 d1 31 00 05 00 01 4c ac
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	Microsoft Secure Server Authority,...
Valid from	02 November 2009 11:22:01 PM
Valid to	02 November 2010 11:22:01 PM
Subject	signup.live.com, Windows Live Op...
Public key	RSA (1024 Bits)
Key Usage	Digital Signature, Key Enciphermen...
SMIME Capabilities	[1]SMIME Capability: Object ID=1....
Enhanced Key Usage	Client Authentication (1.3.6.1.5.5....
Subject Key Identifier	88 69 30 0c 0c 03 9f 68 81 a9 4d 6...
Authority Key Identifier	KeyID=14 55 c4 39 e0 3d 2e d1 55...
CRL Distribution Points	[1]CRL Distribution Point: Distributi...
Authority Information ...	[1]Authority Info Access: Access ...
Certificate Template In...	Template=1.3.6.1.4.1.311.21.8.7...
Application Policies	[1]Application Certificate Policy:Pol...
Thumbprint algorithm	sha1
Thumbprint	a1 f9 b4 95 2f 31 13 40 63 13 9a 3...

MS IE 8.0

### Certificate summary

Holder: signup.live.com, Microsoft Corporation  
 Issuer: Microsoft Secure Server Authority  
 Expires: 02/11/2010 05:52:00 PM GMT

### Encryption protocol

TLS v1.0 128 bit ARC4 (1024 bit RSA/MD5)

Opera 10.60

For creating an account with Hotmail, a user needs to specify a password which is having a minimum of 6 characters in length.

### 1.3 Account Creation – Discussion

In the account creation stage the user is providing sensitive data to the mail providers. Therefore the guarantee of user privacy needs to be with utmost priority. Both the providers go to a great extent to ensure the user's privacy is retained.

Both use HTTPS to establish secured HTTP connections by using Transport layer security (TLS 1.0) which is based on SSL 3.0 [3]

Both providers use RC4 for encryption, in the Cryptanalysis for RC4 performed by Mister & Tavaers [4], RC4 is referred to as *"a secure cipher for practical applications"*.

But RC4 contains weakness, one of which Limor & Hagai[5] describes as

*"The main weakness in this algorithm is that due to a weak key-mixing phase, 1/256 of the keys belong to a class of weak keys. These keys are detectable."*

Several other RC4 weaknesses are described by Andreas Klein [6].

The *RSA/SHA1* hashing algorithm used by Gmail is considered more secure than *RSA/MD-5* hashing algorithm used by Hotmail. Recently MD-5 has been broken and it is also acknowledged by Hotmail Providers [7].

Following are some relative strengths and weaknesses of SHA1 and MD5 [8]

	MD5	SHA-1
<b>Hashing Type</b>	One-way	One-way
<b>Input Data Size</b>	Unlimited	$(2^{64} - 1)$
<b>Hash Value</b>	128-bit	160-bit
<b>Computation Speed</b>	Faster	Slower
<b>Attack Protection</b>	Weaker	Stronger

As the hash value increases, so does the attack protection. Each and every extra bit effectively doubles the time it takes to do a brute-force hack [9]

With the ever increasing computing resources, much difference in computation speed is not noticed by the client side, but it has a profound effect on the server performance. Despite the additional load on the Gmail servers, both providers can be considered achieving high availability.

Hotmail's shorter password length is easier for the users to remember. Password length can be considered proportional to the security strength. But security measures like password hacker bot protection using methods like Captcha (both providers have) and stronger password storage algorithms can achieve a high degree of security even with short passwords.

## **2. User Authentication**

### **2.1 Gmail**

By default a secured connection is established with Gmail when a user wants to login. The connection established is a **TLS v1.0 128 bit ARC4 (1024 bit RSA/SHA)** which is equal to the security implemented for Gmail Account creation (Refer Section 1.1). Gmail's mobile login interface is also secured using the same security measures; therefore the authentication credentials are always encrypted and transmitted.

Apart from the secured communication, Gmail provides **remote sign out and information about recent account activity** [10] which can be used to identify possible account hijacks and prevent them. Also recently Gmail introduced a method for **detecting suspicious account activity** [11], which is based on IP based geographical location mapping to find out about possible account hijacks.

Gmail also provides **full session security** by making the full session SSL secured, therefore the privacy and Integrity of the communication with the Gmail servers is maintained at all time.

### **2.2 Hotmail**

By default Hotmail provides a non-encrypted page, which exchanges information with the server in plain text, therefore the exchanged information is valuable for snooping attacks.

But the user can opt to use SSL for login process which contains the same security as Hotmail account creation. Currently Hotmail does not provide full session security like Gmail.

The Hotmail login interface also provides an option called **Single-use code**, which is intended to enable access Hotmail on public computers without providing a password. The service use a code which is communicated to the Hotmail users' mobile, but the service is offered in nearly 20 countries at the time of this document composition.

### **2.3 User Authentication – Discussion**

Gmail's security measures for user authentication and session security is advanced when compared with Hotmail. A major plus point with Gmail is full session security, which ensures all communication is encrypted.

As zdnet.com article discusses [12], Hotmail in the near future will implement some security measures, which are very similar to security measures currently implemented with Gmail.

### 3. Message Authentication

#### 3.1 Gmail

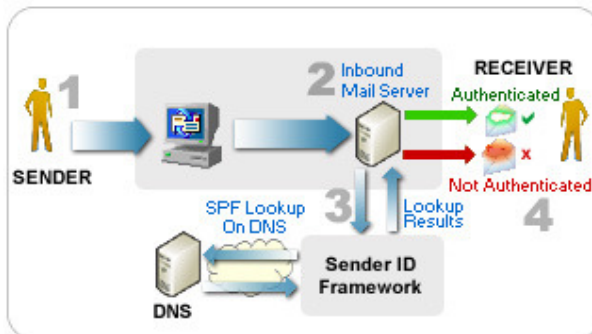
Gmail uses SPF (Sender Policy Framework), DomainKeys, and DKIM (DomainKeys Identified Mail) to authenticate emails [19]. There is an optional feature provided by Gmail, through Google labs, where Gmail marks messages from trusted senders with special symbols, thereby allowing the user to respond to trusted senders [13]. The feature is limited to verifying emails only from PayPal and eBay currently. The following is an extract of Gmail headers of an email sent by Youtube.com which contains authentication information

```
Received-SPF: pass (google.com: domain of service@youtube.com designates 208.65.153.16 as permitted sender) client-ip=208.65.153.16;
DomainKey-Status: good (test mode)
Authentication-Results: mx.google.com; spf=pass (google.com: domain of service@youtube.com designates 208.65.153.16 as permitted sender)
smtp.mail=service@youtube.com; domainkeys=pass (test mode) header.From=service@youtube.com
Received: from sjl-smtp12.sjl.youtube.com (localhost [127.0.0.1])
    by sjl-smtp12.sjl.youtube.com (Postfix) with ESMTP id 8A93A423096D
    for <csudeeraj@gmail.com>; Sat, 7 Aug 2010 18:16:30 -0700 (PDT)
DomainKey-Signature: a=rsa-sha1; b=X9vDuaG0vfnmvLQcFkNkvHieP6ZaA//j3WV2+
3zuczQ+qSwJUokQOs0kUzJxQF0INWgzY/sH34KN38xLXXtJ/SZv6V2WoY8fkYSjvNXURtWmg83nWk6RKroCgdz+qrjgZr3OKBOn2ALtV+
3hDAwHR3oRtUvanAom28S7N+Iw=; c=noaws; d=youtube.com; q=dns; s=selector1
```

#### 3.2 Hotmail

Hotmail uses SIDF (Sender ID Framework) which is based on SPF to authenticate emails, if the sender cannot be authenticated; a warning is displayed [20]. As indicated in the znet.com article [12], future Hotmail updates will include a system for marking mails from trusted senders by special symbols.

Following is a graphical representation of the SIDF extracted from Microsoft.com (Copyright Microsoft)



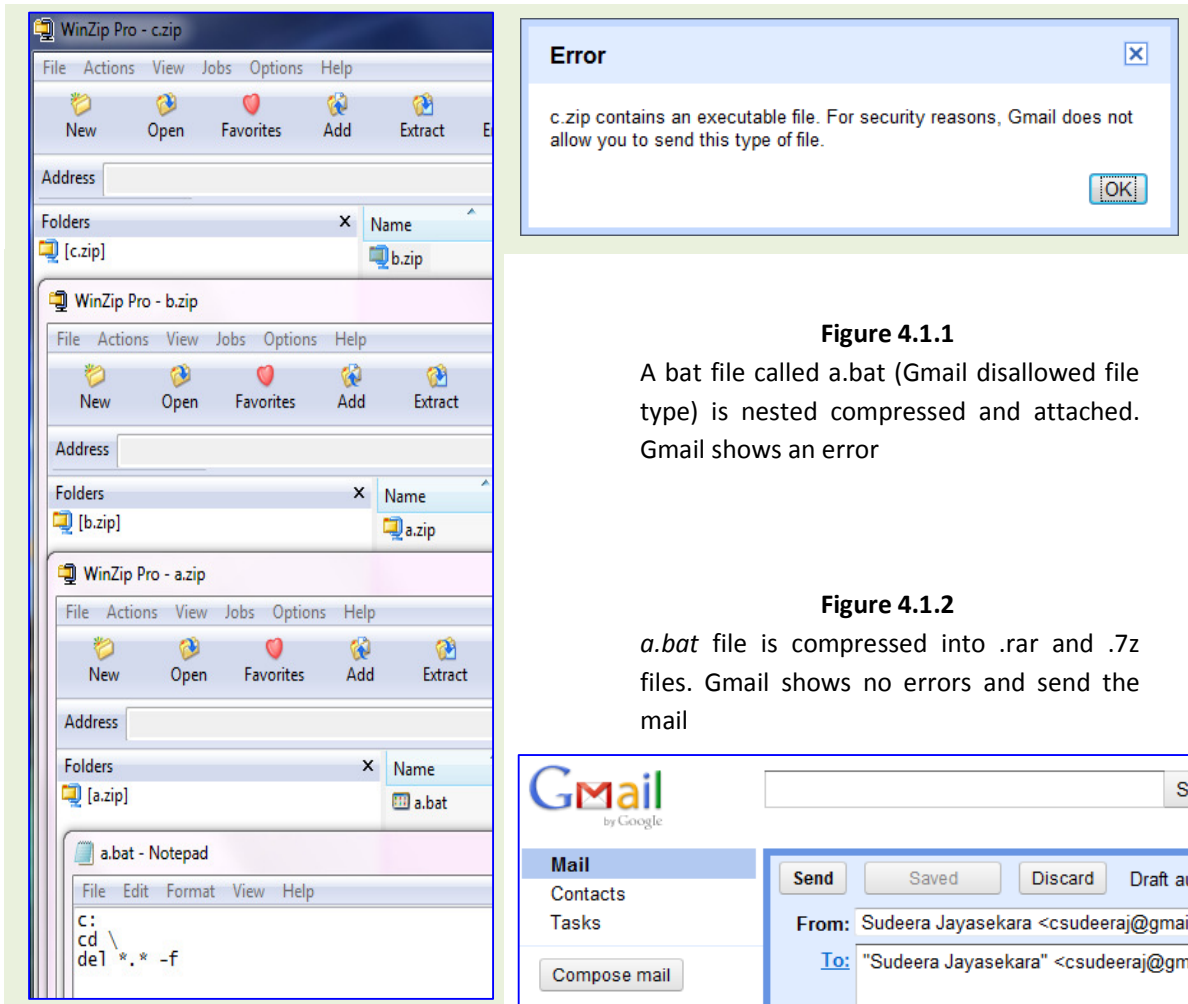
#### 3.3 Message Authentication – Discussion

The widespread usage of message authentication in email providers is to prevent phishing attacks using emails. Both providers provide message authentication, but requires more effort on identifying authenticated senders, with the continuously expanding user base. Both providers lack authentication performed on free email account provider accounts in order to verify the identity of the actual sender.

## 4. Attachment Safety

### 4.1 Gmail

Gmail disallows attaching most file types which could contain malicious code and inflict harm to the receiver [15]. Gmail by default disallows these file types without scanning them for any malicious code, which also prevents a user from sending a safe file of that file type. Gmail also disallows attaching compressed files containing the files of the blocked file types (even nested compressed files are disallowed – figure 4.1.1), but fails to scan and block now popular file types .rar and .7z

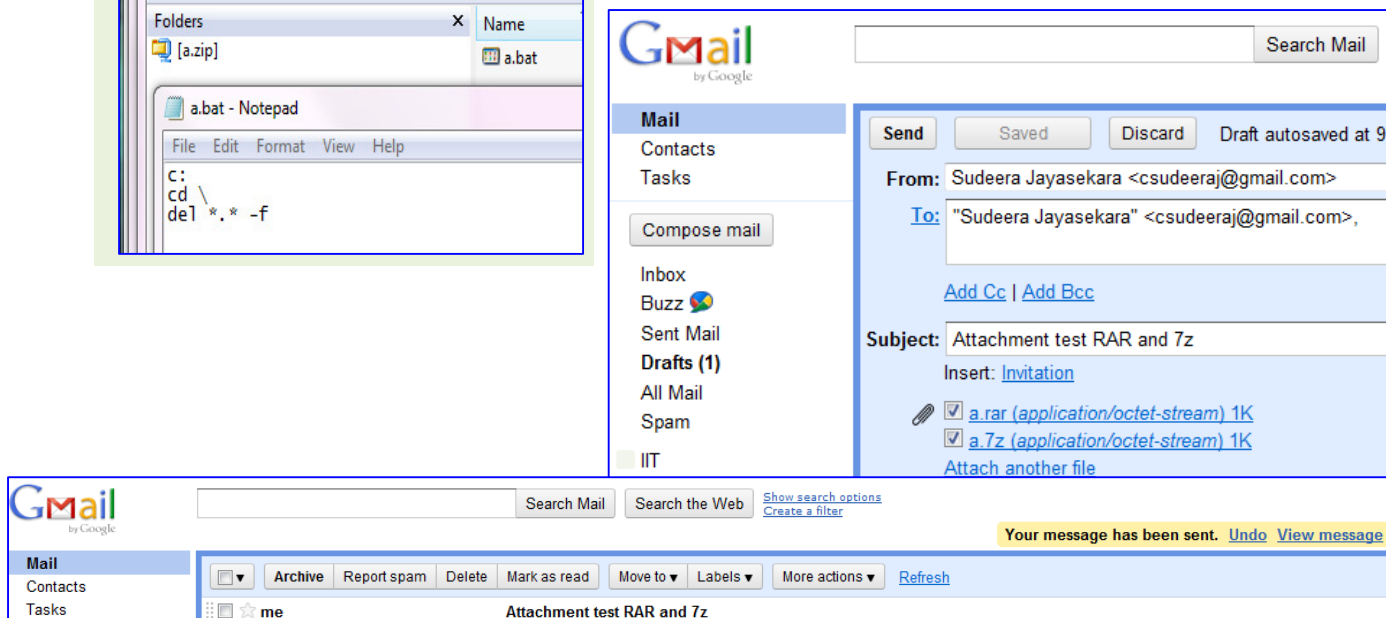


**Figure 4.1.1**

A bat file called a.bat (Gmail disallowed file type) is nested compressed and attached. Gmail shows an error

**Figure 4.1.2**

a.bat file is compressed into .rar and .7z files. Gmail shows no errors and send the mail



Gmail also does not accept any mails containing such attachments. Gmail does not accept such emails from the originating mail servers, raises a delivery failure and returns the following error. *Remote host said: 552 5.7.0 review our attachment guidelines. u3si5311872wfh.36*

This Gmail policy prevents the full e-mail message from getting delivered to the intended Gmail user, not only the attachment. If the sender does not resend the file without the attachment then there is the risk of the Gmail receiver from not receiving an important e-mail.


Gmail's attachment safety has loopholes some of which are published in Amit Agarwal's blog [16], which was published 5 years ago, but ironically all the loopholes mentioned on the blog still exists with Gmail to the time of writing this document.

## 4.2 Hotmail

Like Gmail Hotmail also blocks file types which could contain malicious code. The file types which are blocked are listed in Hotmail documentation. Surprisingly Hotmail itself provides measures of bypassing their attachment filter in the same document. The document states

*"Windows Live Hotmail doesn't support all file types. .... However, to send or receive an unsupported file type as an attachment, use one of the following methods, or ask the person sending you the attachment do so....[methods indicated]*

Not like Gmail, Hotmail does not refuse receiving the full e-mail message if a disallowed file type is present. Hotmail shows the following warning and blocks the individual attachments which the user can unblock if required.

 Attachments, pictures and links in this message have been blocked for your safety. [Show content](#) | [Always show content from this sender](#)

## 4.3 Attachment Safety – Discussion

Gmail has good security measures which ensure attachment safety, which provides some security over malicious attachments. Hotmail has similar security measures. But both providers have exceptional attachment security loop holes. These loopholes are widely known to public and exploited frequently by users, using for malicious and non-malicious activities.

Both providers perform denying of attachments without scanning the attachments properly. This disallows legitimate activity also.

Competitor mail provider Yahoo mail's attachment policy is superior to Gmail and Hotmail. Yahoo mail does not deny some file types by default, but scans each any every file and only prevent attaching files which contain malicious code [18], and this active scanner has been available since year 2000. Yahoo mail also supports (if possible) cleaning files by removing malicious code embedded within.

## 5. Spam Handling

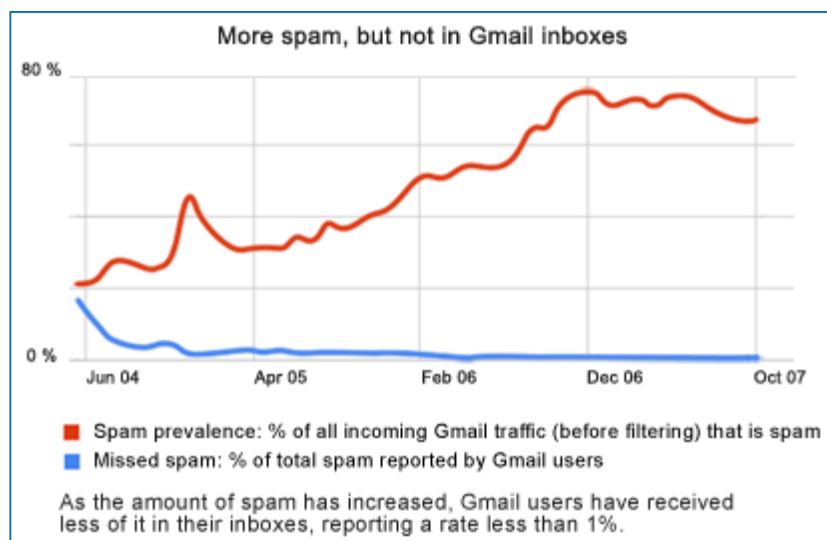
### 5.1 Gmail

Spam filtering in Gmail is done without much user involvement, as Adam Dachis at Lifehacker.com describes [21] this in his article.

Gmail uses the following approaches to identify and filter out Spam using [22],

- Collective information provided by Gmail users reporting spam messages.
- Spam message identification algorithms.
- Other Google technologies adapted to detect spam
- Message authentication (Refer Section 3.1)

The graph is produced by Gmail which indicates their Spam filter efficiency (Copyright Google)



### 5.2 Hotmail

Hotmail uses Microsoft Smart Screen technology to handle Spam. Spam is handled in Hotmail in a similar way to Gmail.

Hotmail filters spam by,

- Using collective information provided by Hotmail users reporting spam messages.
- Scanning message content and performs pattern matching to filter out spam mails.

Hotmail also analyses the user's behavior with messages and identifies potential spam messages which is a feature which Gmail lacks [21].

### 5.3 Spam Handling – Discussion

At the time of writing of this document there is much speculation about a **Fraunhofer Institute** study [23] which concluded that Yahoo Mail and Hotmail have better spam filters than Gmail. Much discussion is presented in the community about the validity of this report [23].

As user who has used all three mail providers Hotmail, Yahoo and Gmail for a considerable amount of time, personally I'm able to conclude that all three mail providers are perform equally well in spam handling. Nether are 100% effective, but all are capable of handling spam mails up to an acceptable level.

## **6. Mail data storage and mail transport**

### **6.1 Gmail**

Gmail offers more than 7 GB of free storage; apart from that fact no information on Gmail mail storage could be collected.

Use of **full session security** (Refer Section 2.1) ensures that the communication between the browser and the Gmail servers are secured. There are also ways like SASL/TLS to encrypt Gmail sent and received through other mail clients using SMTP, IMAP, POP, etc. [24]. Apart from this the security implementations within the Gmail infrastructure could not be collected.

### **6.2 Hotmail**

According to Hotmail the storage of Hotmail is unlimited *“Your inbox capacity will automatically increase as you need more space”* but it depends on the rate of increase of space required by the user [25].

Further information about Hotmail storage could not be collected.

Currently the mail transport between the browser and Hotmail servers are not secured, but there is provision to implement full session security on Hotmail [12]. No further information about Hotmail transport could be collected.

### **6.3 Mail data storage and mail transport – Discussion**

The information in required for this section was unavailable because the information being about the internal structure and internal security implementations which are not publically published by providers.

To ensure full email security in between the sender and receiver (While transport and storage) a utility like PGP could be used to encrypt the email contents.

Employing such a method encrypt sensitive email conversations would be required because both providers scans email messages to display relevant advertisements.

## Conclusion

*Both providers have security mechanisms used to ensure privacy of the user. Gmail seems to be first to implement new security features, but Hotmail is quite quick to follow. Both providers have loopholes, and some security feature lacking, it is evident that both will address these issues in the near future.*

## **References**

- [1] Create an Account  
Gmail  
<https://www.google.com/accounts/NewAccount?service=mail>  
04/08/2010 (access)
- [2] Sign up  
Microsoft  
<https://signup.live.com/signup.aspx?rollrs=12&lic=1>  
04/08/2010 (last access)
- [3] What is TLS/SSL  
Microsoft  
[http://technet.microsoft.com/en-us/library/cc784450\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc784450(WS.10).aspx)  
March 2003
- [4] Cryptanalysis of RC4-like Ciphers  
S. Mister and S. E. Tavares  
[http://target0.be/madchat/crypto/codebreakers/Y\\_23\\_rc4\\_cryptana.pdf](http://target0.be/madchat/crypto/codebreakers/Y_23_rc4_cryptana.pdf)  
1998
- [5] Strength Assessment of Encryption Algorithms  
Limor Elbaz & Hagai Bar-El (Discretix Technologies Ltd.)  
<http://www.discretix.com/PDF/Strength%20Assessment%20of%20Encryption%20Algorithms.pdf>  
October 2000
- [6] Attacks on the RC4 stream cipher  
Andreas Klein  
<http://cage.ugent.be/~klein/RC4/RC4-en.ps>  
February 2006
- [7] Research proves feasibility of collision attacks against MD5 (961509)  
Microsoft Security Advisory  
<http://www.microsoft.com/technet/security/advisory/961509.msp>  
December 2008
- [8] CCNA Security Study Guide  
Tim Boyles  
<http://books.google.lk/books?id=AHzAcvHWbx4C&pg=PA309>  
2010
- [9] A Simple Guide to Cryptography  
Microsoft –MSDN & Wrox Press.  
<http://msdn.microsoft.com/en-us/library/aa480359.aspx>  
1998
- [10] Remote sign out and info to help you protect your Gmail account  
Erwin D'Souza - Gmail  
<http://gmailblog.blogspot.com/2008/07/remote-sign-out-and-info-to-help-you.html>  
July 2008

[11] Detecting suspicious account activity

Pavni Diwanji - Gmail

<http://gmailblog.blogspot.com/2010/03/detecting-suspicious-account-activity.html>

March 2010

[12] Hotmail's new security features vs Gmail's old security features

Dancho Danchev – zdenet.com

<http://www.zdenet.com/blog/security/hotmails-new-security-features-vs-gmails-old-security-features/6509>

May 2010

[13] The super-trustworthy, anti-phishing key

Brad Taylor - Gmail

<http://gmailblog.blogspot.com/2009/07/new-in-labs-super-trustworthy-anti.html>

July 2009

[14] DomainKeys Identified Mail (DKIM)

DKIM

<http://www.dkim.org/>

09/08/2010 (access)

[15] Some file types are blocked

GMail

<http://mail.google.com/support/bin/answer.py?answer=6590>

April 2010

[16] Attach and Send Any File Type with GMail Like EXE, ZIP, Videos; Trick GMail Antivirus Scanner

Amit Agarwal

<http://labnol.blogspot.com/2005/12/cheat-gmail-antivirus-scanner-attach.html>

December 2005

[17] Can't download attachments

Microsoft

[http://help.live.com/Help.aspx?market=en-US&project=MailFull&querytype=topic&query=WL\\_Mail\\_TROU\\_CantDownload.htm](http://help.live.com/Help.aspx?market=en-US&project=MailFull&querytype=topic&query=WL_Mail_TROU_CantDownload.htm)

09/08/2010 (access)

[18] Yahoo! Mail introduces new virus scan feature

Yahoo!

<http://docs.yahoo.com/docs/pr/release517.html>

May 2000

[19] Gmail uses Google's innovative technology to keep spam out of your inbox.

Gmail

<http://www.google.com/mail/help/fightspam/spamexplained.html>

10/08/2010 (access)

[20] MSN Hotmail Adds Safety E-Alerts for E-Mail Authentication

Microsoft

<http://www.microsoft.com/presspass/features/2005/jun05/06-22senderid.msp>

June 2005

[21] How Does the New Hotmail Stack Up to Gmail?

Adam Dachis- Liferhacker.com

<http://liferhacker.com/5564776/how-does-the-new-hotmail-stack-up-to-gmail>

[22] Gmail uses Google's innovative technology to keep spam out of your inbox.

Gmail

<http://www.google.com/mail/help/fightspam/spamexplained.html>

10/08/2010 (access)

[23] Gmail's Spam Filter No Longer Effective?

Alex Chitu – Google system blog

<http://googlesystem.blogspot.com/2010/05/gmails-spam-filter-no-longer-effective.html>

10/08/2010 (access)

[24] GMail and SSL Encryption - how much is encrypted

SuperUser.com

<http://superuser.com/questions/25658/gmail-and-ssl-encryption-how-much-is-encrypted>

11/08/2010 (access)

[25] About your e-mail storage

Hotmail

<http://explore.live.com/windows-live-hotmail-email-storage-about-ui>

11/08/2010 (access)