A statistical analysis of large passwords lists, used to optimize brute force attacks

R.P. van Heerden, J.S. Vorster
CSIR, Pretoria, South Africa
rvheerden@csir.co.za
jvorster@csir.co.za

Abstract: The use of passwords has become endemic in everyday life, and passwords have penetrated most aspects of modern life. The purpose of this paper was to investigate the types of information that can be deduced from password lists, where such lists can be obtained and whether the information obtained can be used to aid brute force password attacks. The World Wide Web and other Internet related search methods were used to obtain password lists. We found that Peer to Peer networks have the most information available. From previous studies and the World Wide Web, the ten most popular passwords from different systems were obtained. Not surprisingly, “password” , “123” and “abc” were found to be the most common passwords. We also obtained the default passwords used by hardware manufacturers from the World Wide Web.

The availability of password lists, their basic structure, the most popular passwords and the frequency of character use were investigated. We investigated the possibility of a more efficient method for cracking passwords by using password statistics. Password statistics and patterns were deduced from a password data set: consisting of 46000 MySpace passwords. The 46000 MySpace usernames and passwords were released late in 2007 after the discovery of a security flaw in MySpace.

The rate at which passwords can be decoded (or cracked) was calculated for different character sets. The most common characters and character sequences were used to optimise brute force password cracking. This method was compared to normal brute force techniques. We concluded that this relationship can be used to optimise a brute force password cracking system in very limited situations.

Passwords are used as the first line of defence in information systems. Thus more effective attack and defence strategies can be developed with a better understanding of the overall statistical properties of passwords. Passwords were demonstrated to be a flawed security mechanism.

Keywords: Passwords

1. Introduction

Technology has evolved to a level where systems using passwords have become an essential part of modern daily life. Passwords have been used from the start of the computer age. One of the first password schemes was implemented by Robert Morris (Morris 1965). He used the “crypt” algorithm, which is based on DES (Data Encryption Standard), with variations to reduce the complexity of the key search.

Computer password use has grown to include access control to software systems such as email, web access and corporate information sites. All of these sites assume that its password is secret. For a password to be useful, the user must be able to remember the password. Increasing the number of passwords required for a user increases the likelihood that the same password would be reused. Thus by compromising a less secure password, a more secure password can be obtained, because a user uses the same password repeatedly.

2. Password lists

We investigated the availability of password lists and their content. Password lists have been the subject of Hollywood movies and other internet myths. In the movie “Hackers” (Wang 1997) , the characters discuss popular passwords as follows:

```
PHREAK
Alright, what are the three most commonly used
passwords?

JOEY
Love, secret, and uh, sex.  But not in that
order, necessarily, right?
```

2.1 Locating Password lists

Password lists were located through the Internet by two methods:

- Internet search engines
- Peer to Peer networks

2.1.1 Internet search engines

The three most popular search engines are (Nielsen 2008):

- Google
- Yahoo
- MSN

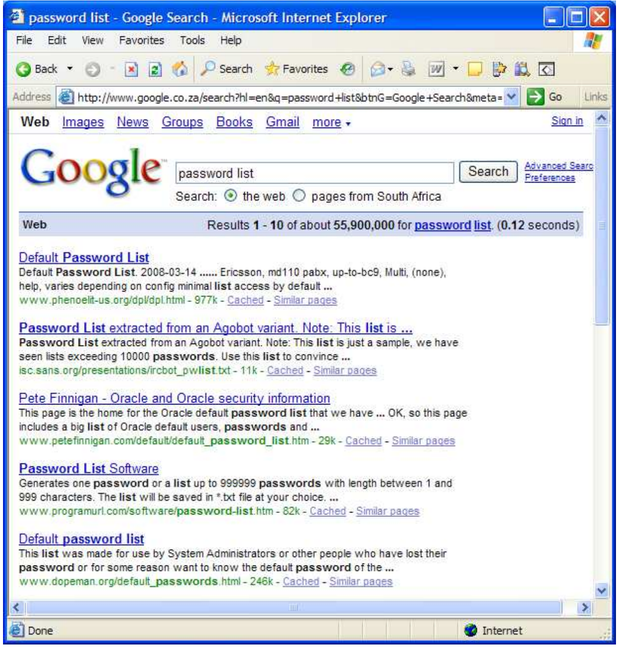
The word “password” is commonly used on internet sites for content control. Thus searching for “password lists” on internet sites returned a huge number of results. Google, Yahoo and MSN returned 55 900 000, 1 380 000 000 and 437 000 000 web sites which conform to “password list” (van Heerden 2008). These numbers far exceed the number of web sites that contain actual password lists. The nature of the search terms does not lend itself to useful results.

In Figure 1, 2 and 3 the results for “password list” are shown.

The search parameters can be refined as follows:

- Specifying that a single phrase is used
- Only look for English web sites
- Only text files.

With these extra specifications the search results were reduced to 988 results. Although it is still a significant number of results, the results are more manageable. The results for a specified search are shown in Figure 4.



password list - Google Search - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links
Web Images News Groups Books Gmail more
Sign in
Google
Search
Advanced Searc
Preferences
Search: ● the web ○ pages from South Africa
Done
Internet

http://www.google.co.za/search?hl=en&q=password+list&btnG=Google+Search&meta=

password list

Web Results **1** - **10** of about **55,900,000** for **password list**. (**0.12** seconds)

Default **Password List**
Default **Password List**. 2008-03-14 ...... Ericsson, md110 pabx, up-to-bc9, Multi, (none), help, varies depending on config minimal **list** access by default **...**
www.phenoelit-us.org/dpl/dpl.html - 977k - Cached - Similar pages

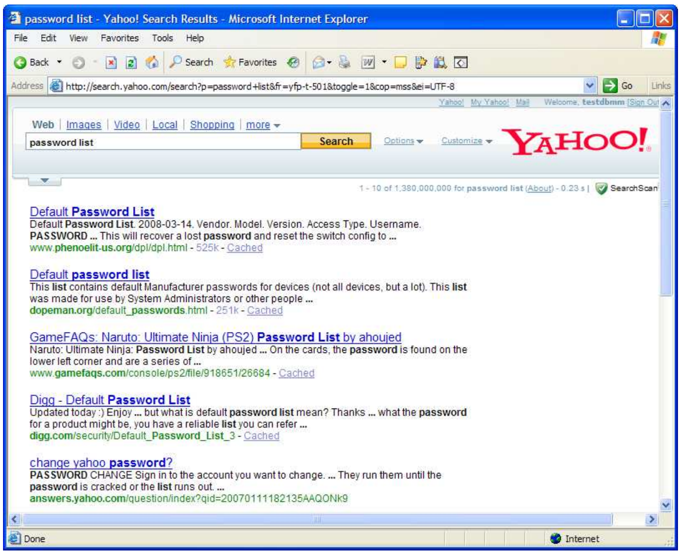
Password List extracted from an Agobot variant. Note: This **list** is **...**
Password List extracted from an Agobot variant. Note: This **list** is just a sample, we have seen lists exceeding 10000 **passwords**. Use this **list** to convince **...**
isc.sans.org/presentations/ircbot_pw**list**.txt - 11k - Cached - Similar pages

Pete Finnigan - Oracle and Oracle security information
This page is the home for the Oracle default **password list** that we have **...** OK, so this page includes a big **list** of Oracle default users, **passwords** and **...**
www.petefinnigan.com/default/default_**password_list**.htm - 29k - Cached - Similar pages

Password List Software
Generates one **password** or a **list** up to 999999 **passwords** with length between 1 and 999 characters. The **list** will be saved in *.txt file at your choice. **...**
www.programurl.com/software/**password-list**.htm - 82k - Cached - Similar pages

Default **password list**
This **list** was made for use by System Administrators or other people who have lost their **password** or for some reason want to know the default **password** of the **...**
www.dopeman.org/default_**passwords**.html - 246k - Cached - Similar pages

Figure 1: Google response to “password list”.


password list - Yahoo! Search Results - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://search.yahoo.com/search?p=password+list&fr=yfp-t-501&toggle=1&cop=mss&ei=UTF-8
Go Links
Yahoo! My Yahoo! Mail Welcome, testdbmm [Sign Out
Web | Images | Video | Local | Shopping | more
password list
Search
Options Customize
YAHOO!
SearchScan
Done
Internet

1 - 10 of 1,380,000,000 for **password list** (About) - 0.23 s |

Default **Password List**
Default **Password List**. 2008-03-14. Vendor. Model. Version. Access Type. Username. **PASSWORD ...** This will recover a lost **password** and reset the switch config to **...**
www.**phenoelit-us.org**/dpl/dpl.html - 525k - Cached

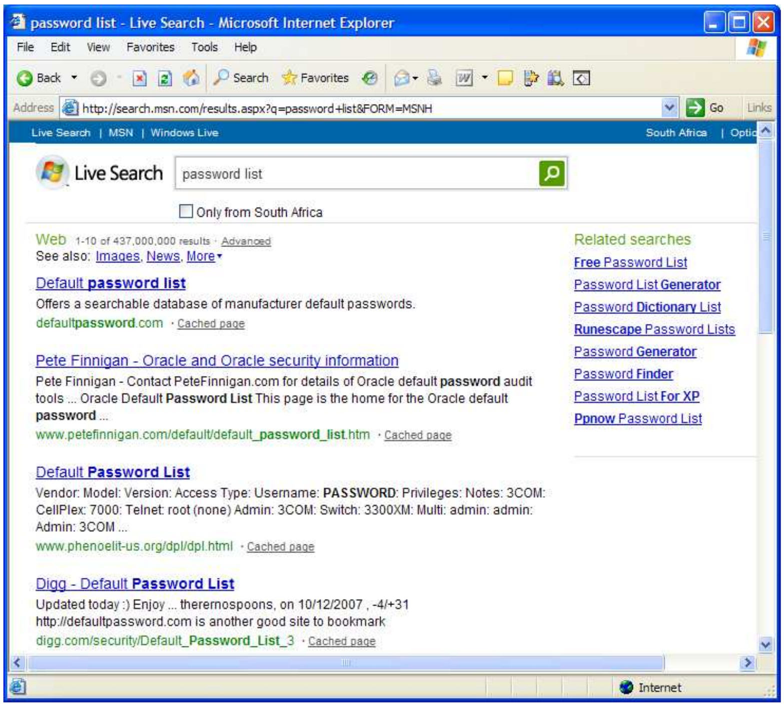
Default **password list**
This **list** contains default Manufacturer passwords for devices (not all devices, but a lot). This **list** was made for use by System Administrators or other people **...**
dopeman.org/default_**passwords**.html - 251k - Cached

GameFAQs: Naruto: Ultimate Ninja (PS2) **Password List** by ahoujed
Naruto: Ultimate Ninja: **Password List** by ahoujed **...** On the cards, the **password** is found on the lower left corner and are a series of **...**
www.**gamefaqs.com**/console/ps2/file/918651/26684 - Cached

Digg - Default **Password List**
Updated today :) Enjoy **...** but what is default **password list** mean? Thanks **...** what the **password** for a product might be, you have a reliable **list** you can refer **...**
digg.com/security/Default_**Password**_**List**_3 - Cached

change yahoo **password**?
PASSWORD CHANGE Sign in to the account you want to change. **...** They run them until the **password** is cracked or the **list** runs out. **...**
answers.yahoo.com/question/index?qid=20070111182135AAQONk9

Figure 2:Yahoo response to “password list”.


password list - Live Search - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://search.msn.com/results.aspx?q=password+list&FORM=MSNH
Go Links
Live Search | MSN | Windows Live
South Africa | Optic
Live Search
password list
□ Only from South Africa
Internet

Web 1-10 of 437,000,000 results · Advanced
See also: Images, News, More

Default **password list**
Offers a searchable database of manufacturer default passwords.
default**password**.com · Cached page

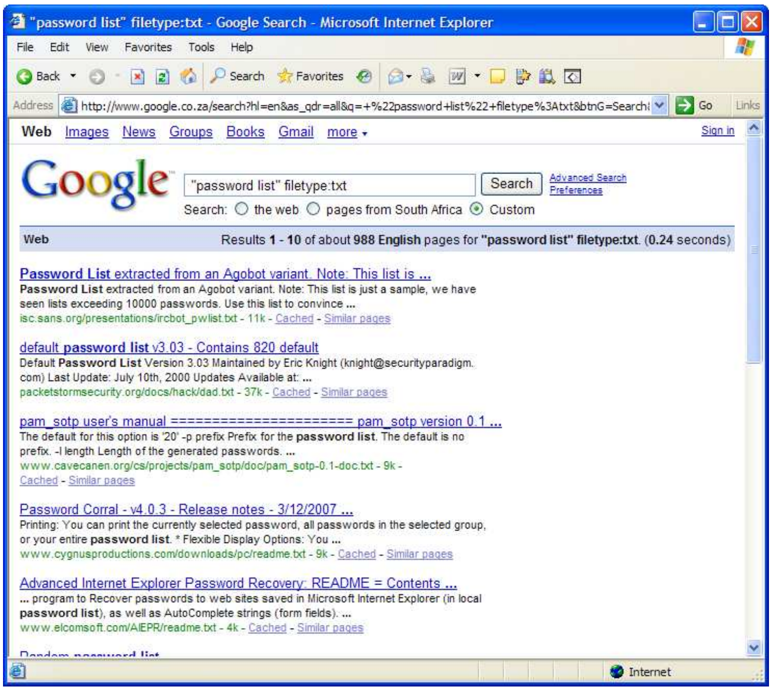
Pete Finnigan - Oracle and Oracle security information
Pete Finnigan - Contact PeteFinnigan.com for details of Oracle default **password** audit tools ... Oracle Default **Password List** This page is the home for the Oracle default **password** ...
www.petefinnigan.com/default/default_**password**_**list**.htm · Cached page

Default **Password List**
Vendor: Model: Version: Access Type: Username: **PASSWORD**: Privileges: Notes: 3COM: CellPlex: 7000: Telnet: root (none) Admin: 3COM: Switch: 3300XM: Multi: admin: admin: Admin: 3COM ...
www.phenoelit-us.org/dpl/dpl.html · Cached page

Digg - Default **Password List**
Updated today :) Enjoy ... therernospoons, on 10/12/2007 , -4/+31 http://defaultpassword.com is another good site to bookmark
digg.com/security/Default_**Password**_**List**_3 · Cached page

Related searches
Free **Password List**
Password List Generator
Password Dictionary List
Runescape Password Lists
Password Generator
Password Finder
Password List For XP
Ppnow Password List

Figure 3: MSN response to “password list”.


"password list" filetype:txt - Google Search - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.google.co.za/search?hl=en&as_qdr=all&q=+%22password+list%22+filetype%3Atxt&btnG=Search
Go
Links
Web Images News Groups Books Gmail more
Sign in
Google
"password list" filetype:txt
Search
Advanced Search
Preferences
Search: ○ the web ○ pages from South Africa ● Custom
Internet

Web Results **1** - **10** of about **988 English** pages for **"password list" filetype:txt**. (**0.24** seconds)

Password List extracted from an Agobot variant. Note: This list is ...
Password List extracted from an Agobot variant. Note: This list is just a sample, we have seen lists exceeding 10000 passwords. Use this list to convince ...
isc.sans.org/presentations/ircbot_pwlist.txt - 11k - Cached - Similar pages

default **password list** v3.03 - Contains 820 default
Default **Password List** Version 3.03 Maintained by Eric Knight (knight@securityparadigm. com) Last Update: July 10th, 2000 Updates Available at: ...
packetstormsecurity.org/docs/hack/dad.txt - 37k - Cached - Similar pages

pam_sotp user's manual ===================== pam_sotp version 0.1 ...
The default for this option is '20' -p prefix Prefix for the **password list**. The default is no prefix. -l length Length of the generated passwords. ...
www.cavecanen.org/cs/projects/pam_sotp/doc/pam_sotp-0.1-doc.txt - 9k - Cached - Similar pages

Password Corral - v4.0.3 - Release notes - 3/12/2007 ...
Printing: You can print the currently selected password, all passwords in the selected group, or your entire **password list**. * Flexible Display Options: You ...
www.cygnusproductions.com/downloads/pc/readme.txt - 9k - Cached - Similar pages

Advanced Internet Explorer Password Recovery: README = Contents ...
... program to Recover passwords to web sites saved in Microsoft Internet Explorer (in local **password list**), as well as AutoComplete strings (form fields). ...
www.elcomsoft.com/AIEPR/readme.txt - 4k - Cached - Similar pages

Random password list

Figure 4: Google response to "password list" with constraints.

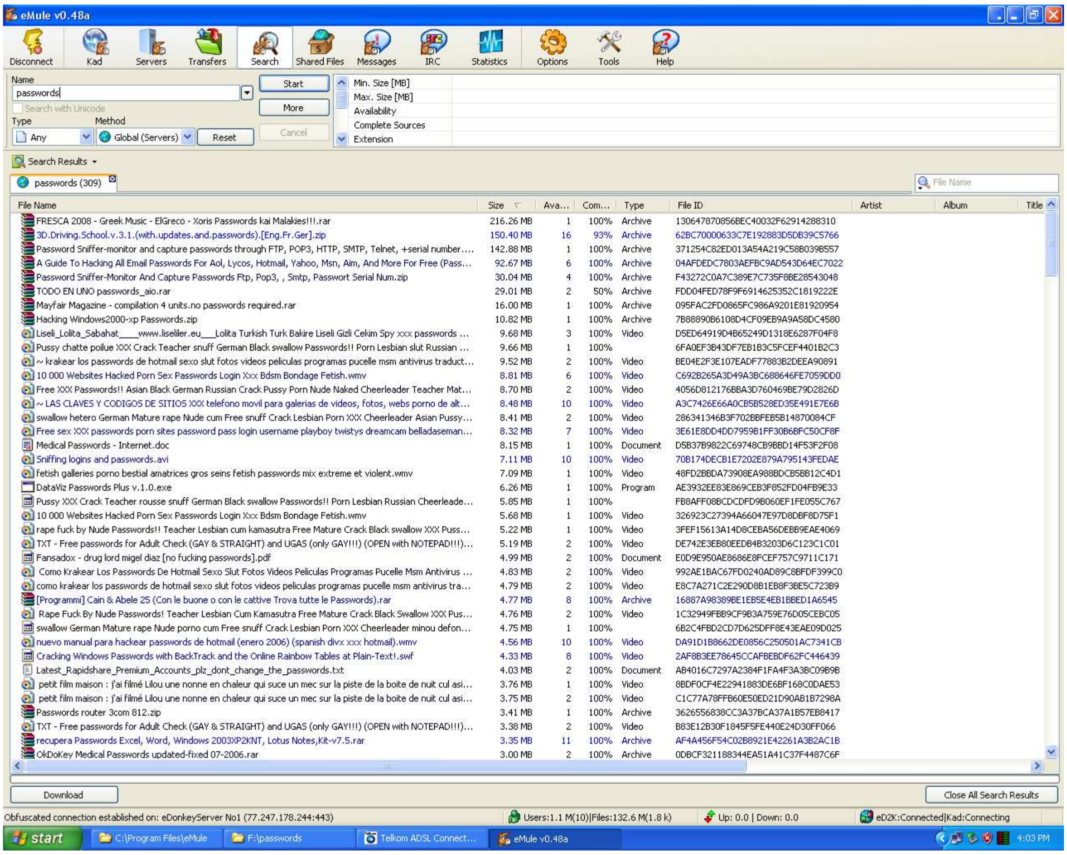
The most common password lists found using Internet search engines were default password lists. These lists contain passwords used by hardware manufacturers as the default security setting.

The SANS (SysAdmin, Audit, Network, Security) Institute password list was one of the first search results obtained. Apart from that the SANS list and default password lists, no other significant password lists were obtained through the Internet search engines used.

2.1.2 Peer to Peer Networks

A Peer to Peer (P2P) network is defined as a network consisting of multiple connected hosts sharing the hosting and bandwidth (Golle 2001). P2P networks form a diversified front, and is therfore relative resistant to any traditional method of assault.

We used a popular P2P software eMule to look for password lists. In Figure 5 and Figure 6, the eMule results for "passwords" is shown (van Heerden 2008).



Name: passwords

Type: Any

Method: Global (Servers)

passwords (309)

File Name	Size	Ava...	Com...	Type	File ID	Artist	Album	Title
FRESCA 2008 - Greek Music - ElGreco - Xoris Passwords kai Malakies!!!.rar	216.26 MB	1	100%	Archive	130647870856BEC40032F62914288310			
3D.Driving.School.v.3.1.(with.updates.and.passwords).[Eng.Fr.Ger].zip	150.40 MB	16	93%	Archive	62BC70000633C7E192883D5DB39C5766			
Password Sniffer-monitor and capture passwords through FTP, POP3, HTTP, SMTP, Telnet, +serial number....	142.88 MB	1	100%	Archive	371254C82ED013A54A219C58B039B557			
A Guide To Hacking All Email Passwords For Aol, Lycos, Hotmail, Yahoo, Msn, Aim, And More For Free (Pass...	92.67 MB	6	100%	Archive	04AFDEDC7803AEFBC9AD543D64EC7022			
Password Sniffer-Monitor And Capture Passwords Ftp, Pop3, , Smtp, Passwort Serial Num.zip	30.04 MB	4	100%	Archive	F43272C0A7C389E7C735F8BE28543048			
TODO EN UNO passwords_aio.rar	29.01 MB	2	50%	Archive	FDD04FED78F9F6914625352C1819222E			
Mayfair Magazine - compilation 4 units.no passwords required.rar	16.00 MB	1	100%	Archive	095FAC2FD0865FC986A9201E81920954			
Hacking Windows2000-xp Passwords.zip	10.82 MB	1	100%	Archive	7B88890B6108D4CF09EB9A9A58DC4580			
Liseli_Lolita_Sabahat____www.liseliler.eu___Lolita Turkish Turk Bakire Liseli Gizli Cekim Spy xxx passwords ...	9.68 MB	3	100%	Video	D5ED64919D4B65249D1318E6287F04F8			
Pussy chatte poilue XXX Crack Teacher snuff German Black swallow Passwords!! Porn Lesbian slut Russian ...	9.66 MB	1	100%		6FA0EF3B43DF7EB1B3C5FCEF4401B2C3			
~ krakear los passwords de hotmail sexo slut fotos videos peliculas programas pucelle msm antivirus traduct...	9.52 MB	2	100%	Video	BE04E2F3E107EADF77883B2DEEA90891			
10 000 Websites Hacked Porn Sex Passwords Login Xxx Bdsm Bondage Fetish.wmv	8.81 MB	6	100%	Video	C692B265A3D49A3BC688646FE7059DD0			
Free XXX Passwords!! Asian Black German Russian Crack Pussy Porn Nude Naked Cheerleader Teacher Mat...	8.70 MB	2	100%	Video	4056D812176BBA3D760469BE79D2826D			
~ LAS CLAVES Y CODIGOS DE SITIOS XXX telefono movil para galerias de videos, fotos, webs porno de alt...	8.48 MB	10	100%	Video	A3C7426E66A0CB5B528ED35E491E7E6B			
swallow hetero German Mature rape Nude cum Free snuff Crack Lesbian Porn XXX Cheerleader Asian Pussy...	8.41 MB	2	100%	Video	286341346B3F702BBFEB5B14870084CF			
Free sex XXX passwords porn sites password pass login username playboy twistys dreamcam belladaseman...	8.32 MB	7	100%	Video	3E61E8DD4DD7959B1FF30B6BFC50CF8F			
Medical Passwords - Internet.doc	8.15 MB	1	100%	Document	D5B37B9822C69748CB9BBD14F53F2F08			
Sniffing logins and passwords.avi	7.11 MB	10	100%	Video	70B174DECB1E7202E879A795143FEDAE			
fetish galleries porno bestial amatrices gros seins fetish passwords mix extreme et violent.wmv	7.09 MB	1	100%	Video	48FD2BBDA73908EA988BDCB5BB12C4D1			
DataViz Passwords Plus v.1.0.exe	6.26 MB	1	100%	Program	AE3932EE83E869CEB3F852FD04FB9E33			
Pussy XXX Crack Teacher rousse snuff German Black swallow Passwords!! Porn Lesbian Russian Cheerleade...	5.85 MB	1	100%		FB8AFF08BCDCDFD9B060EF1FE055C767			
10 000 Websites Hacked Porn Sex Passwords Login Xxx Bdsm Bondage Fetish.wmv	5.68 MB	1	100%	Video	326923C27394A66047E97D8DBF8D75F1			
rape fuck by Nude Passwords!! Teacher Lesbian cum kamasutra Free Mature Crack Black swallow XXX Puss...	5.22 MB	1	100%	Video	3FEF15613A14D8CEBA56DEBB9EAE4069			
TXT - Free passwords for Adult Check (GAY & STRAIGHT) and UGAS (only GAY!!!) (OPEN with NOTEPAD!!!)...	5.19 MB	2	100%	Video	DE742E3EB80EEDB4B3203D6C123C1C01			
Fansadox - drug lord migel diaz [no fucking passwords].pdf	4.99 MB	2	100%	Document	E0D9E950AE8686E8FCEF757C9711C171			
Como Krakear Los Passwords De Hotmail Sexo Slut Fotos Videos Peliculas Programas Pucelle Msm Antivirus ...	4.83 MB	2	100%	Video	992AE1BAC67FD0240AD89C8BFDF399C0			
como krakear los passwords de hotmail sexo slut fotos videos peliculas programas pucelle msm antivirus tra...	4.79 MB	2	100%	Video	E8C7A271C2E290D8B1EB8F3BE5C723B9			
[Programmi] Cain & Abele 25 (Con le buone o con le cattive Trova tutte le Passwords).rar	4.77 MB	8	100%	Archive	16887A98389BE1EB5E4EB1BBED1A6545			
Rape Fuck By Nude Passwords! Teacher Lesbian Cum Kamasutra Free Mature Crack Black Swallow XXX Pus...	4.76 MB	2	100%	Video	1C32949FBB9CF9B3A759E76D05CEBC05			
swallow German Mature rape Nude porno cum Free snuff Crack Lesbian Porn XXX Cheerleader minou defon...	4.75 MB	1	100%		6B2C4FBD2CD7D625DFF8E43EAE09D025			
nuevo manual para hackear passwords de hotmail (enero 2006) (spanish divx xxx hotmail).wmv	4.56 MB	10	100%	Video	DA91D1B8662DE0856C250501AC7341CB			
Cracking Windows Passwords with BackTrack and the Online Rainbow Tables at Plain-Text!.swf	4.33 MB	8	100%	Video	2AF8B3EE78645CCAFBEBDF62FC446439			
Latest_Rapidshare_Premium_Accounts_plz_dont_change_the_passwords.txt	4.03 MB	2	100%	Document	AB4016C7297A2384F1FA4F3A3BC09B9B			
petit film maison : j'ai filmé Lilou une nonne en chaleur qui suce un mec sur la piste de la boite de nuit cul asi...	3.76 MB	1	100%	Video	8BDF0CF4E22941883DE6BF168C0DAE53			
petit film maison : j'ai filmé Lilou une nonne en chaleur qui suce un mec sur la piste de la boite de nuit cul asi...	3.75 MB	2	100%	Video	C1C77A78FFB60E50ED21D90AB1B7298A			
Passwords router 3com 812.zip	3.41 MB	1	100%	Archive	3626556838CC3A37BCA37A1B57EB8417			
TXT - Free passwords for Adult Check (GAY & STRAIGHT) and UGAS (only GAY!!!) (OPEN with NOTEPAD!!!)...	3.38 MB	2	100%	Video	B83E12B30F1845F5FE440E24D30FF066			
recupera Passwords Excel, Word, Windows 2003XP2KNT, Lotus Notes,Kit-v7.5.rar	3.35 MB	11	100%	Archive	AF4A456F54C02B8921E42261A3B2AC1B			
OkDoKey Medical Passwords updated-fixed 07-2006.rar	3.00 MB	2	100%	Archive	0DBCF321188344EA51A41C37F4487C6F			

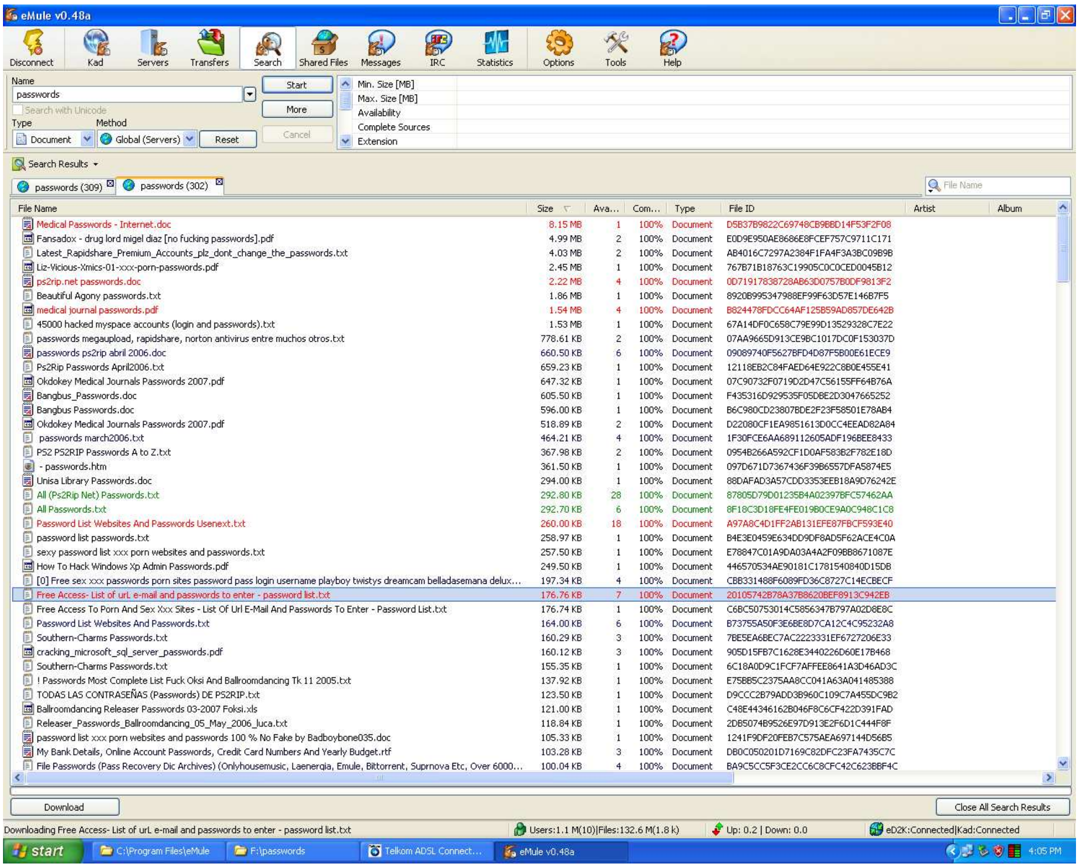
Obfuscated connection established on: eDonkeyServer No1 (77.247.178.244:443)

Users:1.1 M(10)|Files:132.6 M(1.8 k)

Up: 0.0 | Down: 0.0

eD2K:Connected|Kad:Connecting

Figure 5: eMule Search for “passwords”



Name: passwords

Type: Document

Method: Global (Servers)

passwords (309) passwords (302)

File Name	Size	Ava...	Com...	Type	File ID	Artist	Album
Medical Passwords - Internet.doc	8.15 MB	1	100%	Document	D5B37B9822C69748CB9BBD14F53F2F08		
Fansadox - drug lord migel diaz [no fucking passwords].pdf	4.99 MB	2	100%	Document	E0D9E950AE8686E8FCEF757C9711C171		
Latest_Rapidshare_Premium_Accounts_plz_dont_change_the_passwords.txt	4.03 MB	2	100%	Document	AB4016C7297A2384F1FA4F3A3BC09B9B		
Liz-Vicious-Xmics-01-xxx-porn-passwords.pdf	2.45 MB	1	100%	Document	767B71B18763C19905C0C0CED0045B12		
ps2rip.net passwords.doc	2.22 MB	4	100%	Document	0D71917838728AB63D0757B0DF9813F2		
Beautiful Agony passwords.txt	1.86 MB	1	100%	Document	8920B995347988EF99F63D57E146B7F5		
medical journal passwords.pdf	1.54 MB	4	100%	Document	B824478FDCC64AF125B59AD857DE642B		
45000 hacked myspace accounts (login and passwords).txt	1.53 MB	1	100%	Document	67A14DF0C658C79E99D13529328C7E22		
passwords megaupload, rapidshare, norton antivirus entre muchos otros.txt	778.61 KB	2	100%	Document	07AA9665D913CE9BC1017DC0F153037D		
passwords ps2rip abril 2006.doc	660.50 KB	6	100%	Document	09089740F5627BFD4D87F5B00E61ECE9		
Ps2Rip Passwords April2006.txt	659.23 KB	1	100%	Document	12118EB2C84FAED64E922C8B0E455E41		
Okdokey Medical Journals Passwords 2007.pdf	647.32 KB	1	100%	Document	07C90732F0719D2D47C56155FF64B76A		
Bangbus_Passwords.doc	605.50 KB	1	100%	Document	F435316D929535F05DBE2D3047665252		
Bangbus Passwords.doc	596.00 KB	1	100%	Document	B6C980CD23807BDE2F23F58501E78AB4		
Okdokey Medical Journals Passwords 2007.pdf	518.89 KB	2	100%	Document	D22080CF1EA9851613D0CC4EEAD82A84		
passwords march2006.txt	464.21 KB	4	100%	Document	1F30FCE6AA689112605ADF196BEE8433		
PS2 PS2RIP Passwords A to Z.txt	367.98 KB	2	100%	Document	0954B266A592CF1D0AF583B2F782E18D		
- passwords.htm	361.50 KB	1	100%	Document	097D671D7367436F39B6557DFA5874E5		
Unisa Library Passwords.doc	294.00 KB	1	100%	Document	88DAFAD3A57CDD3353EEB18A9D76242E		
All (Ps2Rip Net) Passwords.txt	292.80 KB	28	100%	Document	87805D79D01235B4A02397BFC57462AA		
All Passwords.txt	292.70 KB	6	100%	Document	8F18C3D18FE4FE019B0CE9A0C948C1C8		
Password List Websites And Passwords Usenext.txt	260.00 KB	18	100%	Document	A97A8C4D1FF2AB131EFE87FBCF593E40		
password list passwords.txt	258.97 KB	1	100%	Document	B4E3E0459E634DD9DF8AD5F62ACE4C0A		
sexy password list xxx porn websites and passwords.txt	257.50 KB	1	100%	Document	E78847C01A9DA03A4A2F09BB8671087E		
How To Hack Windows Xp Admin Passwords.pdf	249.50 KB	1	100%	Document	446570534AE90181C1781540840D15DB		
[0] Free sex xxx passwords porn sites password pass login username playboy twistys dreamcam belladasemana delux...	197.34 KB	4	100%	Document	CBB331488F6089FD36C8727C14ECBECF		
Free Access- List of urL e-mail and passwords to enter - password list.txt	176.76 KB	7	100%	Document	20105742B78A37B8620BEF8913C942EB		
Free Access To Porn And Sex Xxx Sites - List Of Url E-Mail And Passwords To Enter - Password List.txt	176.74 KB	1	100%	Document	C6BC50753014C5856347B797A02D8E8C		
Password List Websites And Passwords.txt	164.00 KB	6	100%	Document	B73755A50F3E6BE8D7CA12C4C95232A8		
Southern-Charms Passwords.txt	160.29 KB	3	100%	Document	7BE5EA6BEC7AC2223331EF6727206E33		
cracking_microsoft_sql_server_passwords.pdf	160.12 KB	3	100%	Document	905D15FB7C1628E3440226D60E17B468		
Southern-Charms Passwords.txt	155.35 KB	1	100%	Document	6C18A0D9C1FCF7AFFEE8641A3D46AD3C		
! Passwords Most Complete List Fuck Oksi And Ballroomdancing Tk 11 2005.txt	137.92 KB	1	100%	Document	E75BB5C2375AA8CC041A63A041485388		
TODAS LAS CONTRASEÑAS (Passwords) DE PS2RIP.txt	123.50 KB	1	100%	Document	D9CCC2B79ADD3B960C109C7A455DC9B2		
Ballroomdancing Releaser Passwords 03-2007 Foksi.xls	121.00 KB	1	100%	Document	C48E44346162B046F8C6CF422D391FAD		
Releaser_Passwords_Ballroomdancing_05_May_2006_luca.txt	118.84 KB	1	100%	Document	2DB5074B9526E97D913E2F6D1C444F8F		
password list xxx porn websites and passwords 100 % No Fake by Badboybone035.doc	105.33 KB	1	100%	Document	1241F9DF20FEB7C575AEA697144D56B5		
My Bank Details, Online Account Passwords, Credit Card Numbers And Yearly Budget.rtf	103.28 KB	3	100%	Document	DB0C050201D7169C82DFC23FA7435C7C		
File Passwords (Pass Recovery Dic Archives) (Onlyhousemusic, Laenergia, Emule, Bittorrent, Suprnova Etc, Over 6000...	100.04 KB	4	100%	Document	BA9C5CC5F3CE2CC6C8CFC42C623BBF4C		

Downloading Free Access- List of urL e-mail and passwords to enter - password list.txt

Users:1.1 M(10)|Files:132.6 M(1.8 k)

Up: 0.2 | Down: 0.0

eD2K:Connected|Kad:Connected

Figure 6: eMule Search for “passwords” documents

Results obtained using eMule were more encouraging than that obtained using internet search engines. The following password lists were obtained:

- Unix administrator (root) passwords
- MySpace accounts
- Default password list
- FTP list
- WiFi Access Points Passwords

2.2 Popular password studies

2.2.1 Unix Passwords

Klein attempted to crack 15000 Unix passwords in 1989. He successfully obtained 25% of passwords using a dictionary attack(Klein 1990). The study lasted 12 months, although 80% of the passwords guessed were obtained in the first week. The following trends were revealed:

- The most popular password length is 6 characters with 34.7 % use
- Common names are used in 4% of the passwords
- Username and passwords are the same in 2.7% of passwords
- Cartoons, Movies, fiction and place names are used in 1.4% of passwords

The average computer user has changed significantly since 1989, and thus the password use pattern is expected to change. The following factors can be expected to impact password use today:

- The average computer user has to remember much more computer passwords than in 1989
- More computer illiterate users now use computers
- Computer processing power has increased by at least 500 fold (Geer 2005)

2.2.2 UK Web passwords

Stuart Brown compiled a list of the most popular passwords used for various web sites. The top 10 passwords comprise 6.5% of all the passwords used (Brown 2006). The top ten passwords were:

- 123
- password
- liverpool
- letmein (“let me in”)
- 123456
- qwerty
- charlie
- monkey
- arsenal
- thomas

Some area-specific passwords (liverpool and arsenal) made the top 10 list, along with other common passwords (123456, qwerty, password).

2.2.3 PCMag.com

PC magazine listed their most commonly used passwords as (PCmag 2007):

- password
- 123456
- qwerty
- abc123
- letmein
- monkey
- myspace1
- password1
- bink182
- (username)

The PC magazine list shares some similarities with the Brown list. Exceptions are the use of unique UK area-specific passwords.

2.2.4 J Ruska

Jimmy Ruska constructed a list of passwords from online students (Ruska 2008):

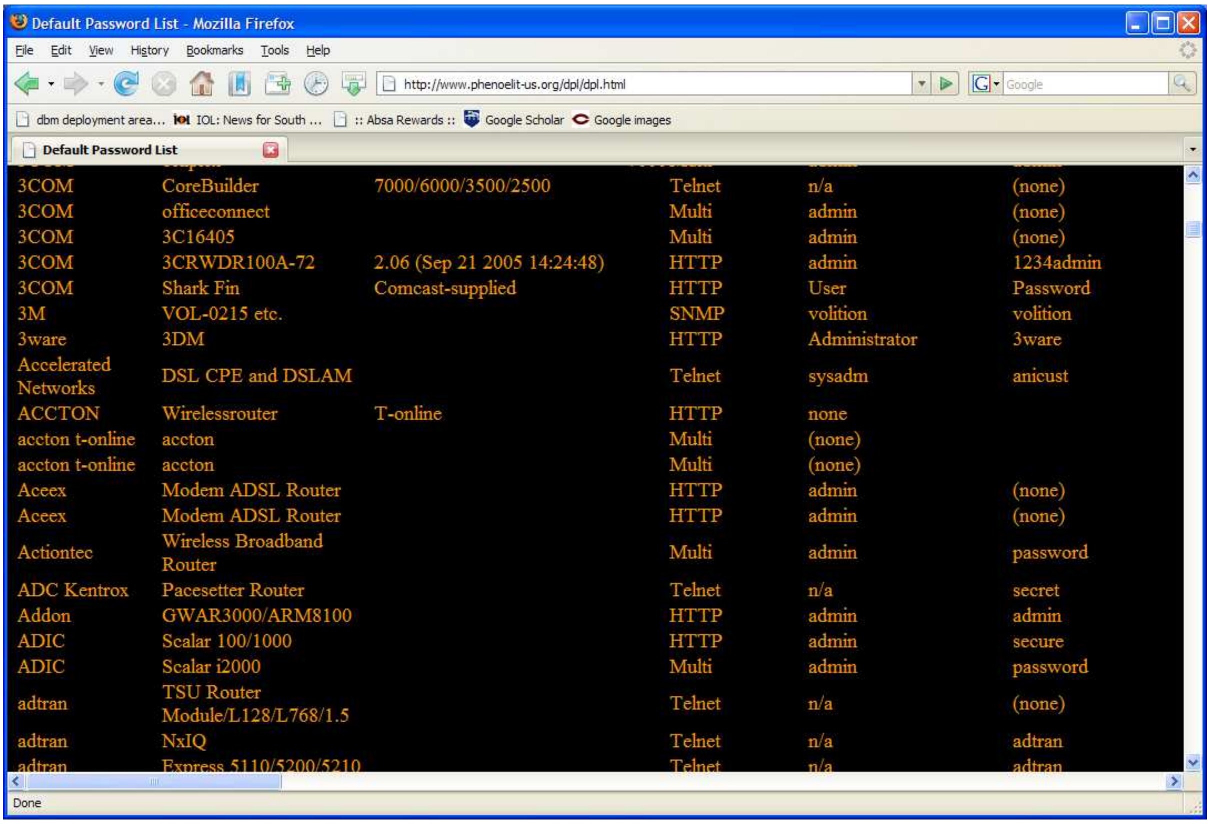
- 123456, 123, 123123, 01234, 2468, 987654, etc
- 123abc, abc123, 246abc
- First Name
- Favourite Band
- Favourite Song
- first letter of given name then surname
- qwerty, asdf, and other keyboard rolls
- Favourite cartoon or movie character
- Favourite sport, or sports star
- Country of origin
- City of origin
- All numbers
- Some word in the dictionary
- Combining 2 dictionary words
- any of the above spelled backwards
- aaa, eee, llll, 999999, and other repeat combinations

2.2.5 Default Passwords

Default passwords for computer hardware were obtained from the following websites:

- Various hardware passwords
  - http://www.securiteam.com/securitynews/5RR080A1TS.html
  - http://www.cirt.net/passwords
  - http://defaultpassword.com/
  - http://www.governmentsecurity.org/articles/DefaultLoginsandPasswordsforNetworkedDevices.php,
- Bios Backdoor passwords
  - http://www.freelabs.com/~whitis/security/backdoor.html
- Switches and Routers
  - http://www.dopeman.org/default_passwords.html
  - http://www.cyxla.com/passwords/passwords.html
  - http://www.routerpasswords.com/
  - http://www.phenoelit-us.org/dpl/dpl.html

Many more websites containing lists of default passwords exist. Thus default passwords for any hardware device can be obtained from the Internet. In Figure 7, an example of a default password list is shown.


Default Password List - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.phenoelit-us.org/dpl/dpl.html
Google
dbm deployment area... IOL: News for South ... :: Absa Rewards :: Google Scholar Google images
Default Password List
Done

3COM	CoreBuilder	7000/6000/3500/2500	Telnet	n/a	(none)
3COM	officeconnect		Multi	admin	(none)
3COM	3C16405		Multi	admin	(none)
3COM	3CRWDR100A-72	2.06 (Sep 21 2005 14:24:48)	HTTP	admin	1234admin
3COM	Shark Fin	Comcast-supplied	HTTP	User	Password
3M	VOL-0215 etc.		SNMP	volition	volition
3ware	3DM		HTTP	Administrator	3ware
Accelerated Networks	DSL CPE and DSLAM		Telnet	sysadm	anicust
ACCTON	Wirelessrouter	T-online	HTTP	none	
accton t-online	accton		Multi	(none)	
accton t-online	accton		Multi	(none)	
Aceex	Modem ADSL Router		HTTP	admin	(none)
Aceex	Modem ADSL Router		HTTP	admin	(none)
Actiontec	Wireless Broadband Router		Multi	admin	password
ADC Kentrox	Pacesetter Router		Telnet	n/a	secret
Addon	GWAR3000/ARM8100		HTTP	admin	admin
ADIC	Scalar 100/1000		HTTP	admin	secure
ADIC	Scalar i2000		Multi	admin	password
adtran	TSU Router Module/L128/L768/1.5		Telnet	n/a	(none)
adtran	NxIQ		Telnet	n/a	adtran
adtran	Express 5110/5200/5210		Telnet	n/a	adtran

Figure 7: Default Password list

3 Passwords Statistics

3.1 Most common passwords

The most popular passwords were collated from the following passwords lists:

- Unix administrator (root) passwords
- MySpace accounts
- Default password lists, WiFi Access Points Passwords
- FTP list

In Table 1 to Table 4 the most common passwords used are listed.

Table 1: Unix administrator (root) passwords, Top 10.

	Password
1	12345
2	abc123
3	password
4	computer
5	123456
6	tigger
7	1234
8	a1b2c3
9	qwerty
10	123

In Table 1, common Unix root passwords include simple (and easily guessed) passwords, such as “password”, “12345” and “qwerty”.

Table 2: MySpace Top 10.

	Password (MySpace)
1	password1
2	abc123
3	password
4	iloveyou1
5	iloveyou2
6	fuckyou1
7	soccer1
8	myspace1
9	iloveyou
10	iloveyou!

In Table 2, the most common passwords include a “1” or “2” character as an end character. The password rules for MySpace accounts changed to force users to use numerical characters in their passwords.

Table 3: Unix, Default, Default2 and WiFi Top 10.

	Password (WiFi)	**Password (Default)**	**Password (Default2)**	**Password (Unix)**
1	admin	admin	admin	12345
2	password	1234	password	abc123
3	sysadm	password	root	password
4	manager	manager	epicrooter	computer
5	system	none	sysadmin	123456
6	1234	system	access	tigger
7	guest	blank	smcadmin	1234
8	root	netman	sysadm	a1b2c3
9	access	Tech	user	qwerty
10	cascade	netman	ADMINISTRATOR	123

The passwords used by hardware manufacturers are very limited. Most of the passwords have an administrator (admin, rootm sysadmin, …) theme. The usual suspect “password” is also very popular. From the list in Table 3, the need to change hardware default passwords becomes apparent. The WiFi passwords correlate with the default passwords, thus indicating that the WiFi access point default passwords have not been changed.

Table 4: FTP, Top 10.

	Password (FTP)
1	leech
2	anonymous
3	mp3
4	leechme
5	mp3
6	warez

7	anon
8	anonymous@user.com
9	L33ch
10	me

The term “leech” refers to downloading, and is inspired from the parasitic leech found in nature. The data available from FTP sites (e.g. mp3, movies and software) often inspire the choice of passwords used.

3.2 Character Frequencies

The frequency of characters were calculated for the passwords in the MySpace password list and compared to an English dictionary of 62000 words.

In Table 5, the character frequencies are shown. The frequencies are similar to that of dictionary file as shown in Table 6.

Table 5: Character Frequencies for MySpace passwords

Rank	**Char**	**Freq (%)**	**Rank**	**Char**	**Freq (%)**	**Rank**	**Char**	**Freq (%)**
1	e	7.5	26	8	1.44	51	B	0.09
2	a	6.81	27	5	1.43	52	*	0.08
3	1	6.31	28	6	1.39	53	D	0.07
4	o	5.35	29	7	1.3	54	H	0.07
5	s	4.69	30	f	1.16	55	Y	0.07
6	i	4.69	31	w	1.04	56	U	0.06
7	r	4.57	32	v	0.99	57	K	0.06
8	l	4.47	33	j	0.87	58	P	0.05
9	n	4.15	34	!	0.52	59	G	0.05
10	t	3.45	35	z	0.41	60	-	0.05
11	2	3.43	36	x	0.39	61	J	0.04
12	c	3.02	37	.	0.3	62	F	0.04
13	m	2.76	38	A	0.19	63	$	0.04
14	y	2.35	39	E	0.18	64	V	0.03
15	d	2.35	40	q	0.15	65	_	0.03
16	b	2.34	41	S	0.14	66	<	0.03
17	h	2.33	42	I	0.13	67	W	0.03
18	3	2.33	43	O	0.13	68	?	0.02
19	0	2.26	44	L	0.12	69	'	0.02
20	u	2.19	45	N	0.11	70	Z	0.02
21	k	1.97	46	R	0.11	71	;	0.01
22	p	1.81	47	\	0.11	72	X	0.01
23	g	1.75	48	C	0.1	73	=	0.01
24	4	1.65	49	T	0.09	74	`	0.01
25	9	1.57	50	M	0.09	75	/	0.01

Table 6: Character Frequencies for Dictionary file

Rank	Char	Freq (%)	Rank	Char	Freq (%)
1	e	11.21	28	x	0.27
2	a	8.53	29	B	0.25
3	i	8.38	30	D	0.19
4	r	7.28	31	L	0.18
5	n	7.16	32	'	0.18
6	t	6.46	33	T	0.18
7	s	6.39	34	R	0.17
8	o	6.35	35	G	0.17
9	l	5.46	36	q	0.17
10	c	3.8	37	P	0.17
11	u	3.18	38	j	0.16
12	d	3.09	39	H	0.16
13	m	2.72	40	E	0.15
14	p	2.56	41	K	0.14
15	h	2.44	42	J	0.12
16	g	2.27	43	N	0.11
17	b	1.91	44	F	0.11
18	y	1.88	45	W	0.1
19	f	1.2	46	O	0.08
20	v	1.02	47	I	0.08
21	k	0.91	48	V	0.07
22	w	0.82	49	U	0.03
23	z	0.41	50	Y	0.03
24	M	0.31	51	Z	0.03
25	C	0.31	52	é	0.02
26	A	0.29	53	Q	0.01
27	S	0.29	54	X	0.01

3.3 Password Length

The lengths of the passwords used by the 46000 MySpace users are plotted in Figure 8 and Figure 9.

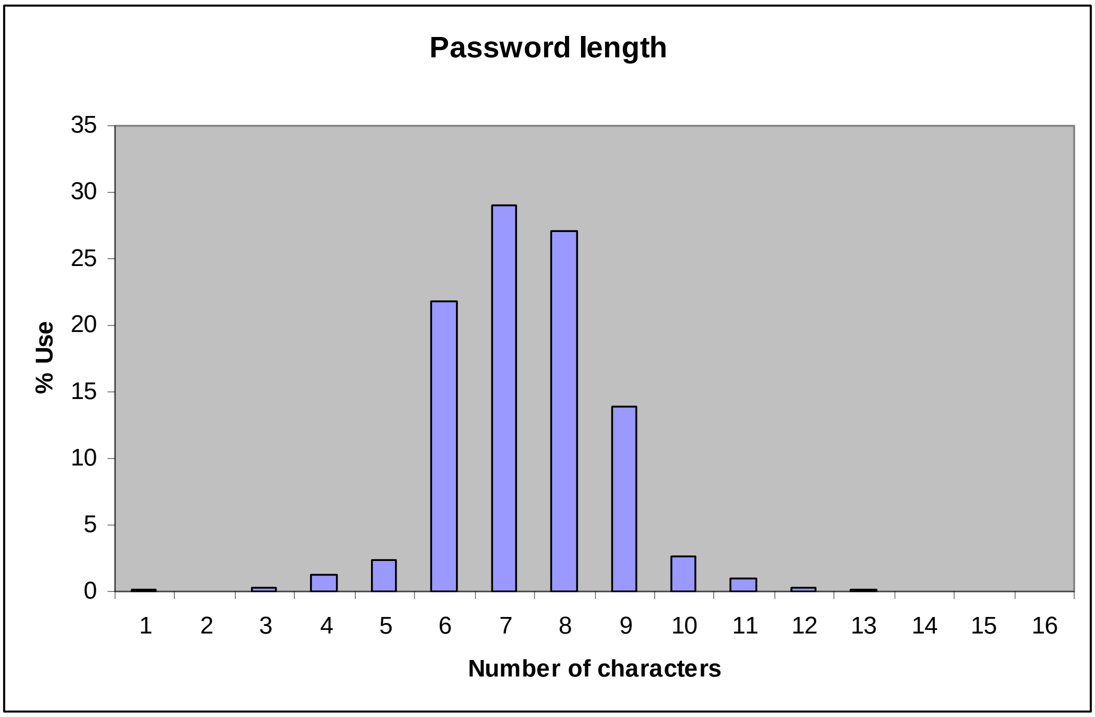


Figure 8: Password Length

As shown in Figure 8, the most popular password length was 6 to 10 characters.

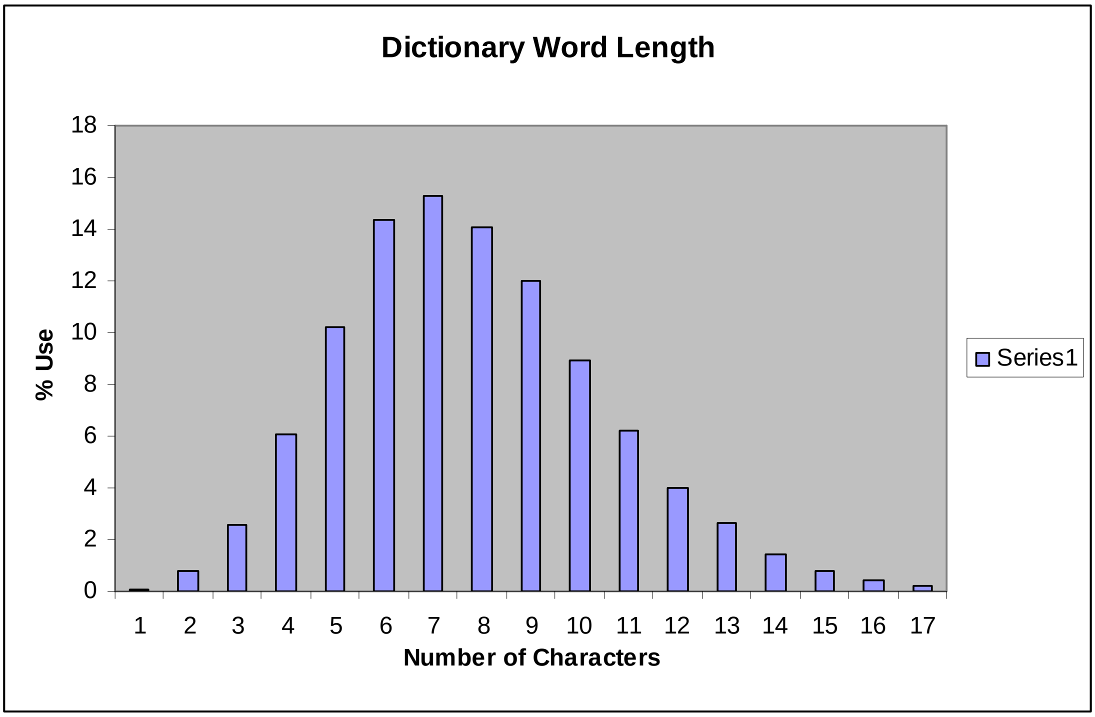


Figure 9: Dictionary length

In Figure 8, the length of words in a common English dictionary is shown. The password length distribution is narrower than the dictionary distribution.

Thus password searches can be optimised to search for passwords of only 6-10 characters in length.

4 Theoretical uses of passwords statistics

4.1 Number of characters used

A password cracker has to crack all possible passwords. Firstly, it will have to attempt all words consisting of only one character, thus: a, b, c, …, z, 0, 1, ..9, !, @, #, $, and so on through the entire list of all possible characters.

Secondly, this the cracker will have to attempt all possible two-character combinations, starting from aa..az, a0..a9, a + all special characters, then moving to ba, bb, … bz, and so on, for each of the characters, ending for example %^, %&, %*, %%.

If there are 100 characters to choose from, there will be 100^2 = 10,000 different combinations with two characters. Thirdly, the cracker will have to attempt all possible three-letter combination to the total number of 1,000,000 different combinations.

Therefore the total amount of combinations a cracker has to consider in order to crack all possible passwords is: (with a character set of 100 characters)

$$100^1 + 100^2 + \ldots + 100^7 = 101{,}010101{,}010100$$

This is roughly equal to 101 million million. This amount of combinations is so enormous that it is not viable to consider them all.

Using a subset rather than all possible characters can reduce the search space. For example only 10 characters. The top 10 used could do, but for the purpose of demonstration, use: a, b, c, d, e, f, g, h, i and j.

If this is the subset, then the password cracker will attempt first: a, b, c, j, and then aa, ab, ac, .. aj, ba, bb, .. bj, ca.. cj, and so on up to ja, jb, … jj. A total of 10*10 = 100 possibilities.

Next, it will attempt all three-letter combinations, and then four, five, six and seven-letter combinations, ending with aaaaaaa… jdfhadf … jjjjjj.

The cracker will then have tried

$$10^1 + 10^2 + 10^3 + \ldots + 10^7 = 11{,}111110$$

Thus a total of just over 11 million permutations.

There seems to be an exponential relation between the number of characters in subset and the amount of time to iterate through all the possible combinations of these characters. This relation is counter-balanced by the smaller range of passwords with reduced character sets.

4. 2 Viability of Statistical reduction password cracking

To test the viability of such a reduction in a character set, a number of different subsets of characters were constructed. Each set had a different number of characters. The only parameter that was measured in this experiment was the amount of time taken to complete all possible combinations.

The “John the Ripper” password decoder was instructed to attempt to crack a huge password file (over 12000 passwords) using each of the character subsets. The time that the cracker took on each run was noted. The passwords were all obtained from Windows NT workstation and thus have a maximum length of 8 characters.

Due to time limitations only character sizes up to 20 was tested. This is not sufficient for characterizing the performance of for larger character sizes.

The results of this test are tabulated in Table 7. For a character length of six or less the cracker software goes through all possible combinations in less than a second. Thus the software reports a time of zero seconds.

***Table 7*:** Time per number of characters.

Number of Characters	Time (m)
1	0.00
2	0.00
3	0.00
4	0.00
5	0.00
6	0.00
7	0.02
8	0.05
9	0.12
10	0.23
11	0.45
12	0.80
13	1.40
14	2.32
15	3.72
16	5.72
17	8.57
18	12.72
19	18.33
20	25.53
21	35.27
22	47.87
23	64.05
24	85.02
25	112.08
26	146.73
27	189.08
28	239.00
29	302.12
30	377.13
31	468.02
32	576.73
33	706.58
34	866.87
35	1055.72
36	1282.45

At 36 characters the cracking process takes 1282.45 minutes (almost 22 hours).

4.3.1 Analysis

In Figure 10, a trend-line has been curve-fitted to the data. The graph follows a power curve. A power curve is a curve wherein the relationship between the dependent and independent variables is given by:

$y = k\, x^{\alpha}$

In this case it seems that the best fitting is where:

$k = 4x10^{-8}$

$\alpha = 6.7579$

As can be seen from the graph the above equations approximate to a very good fit.

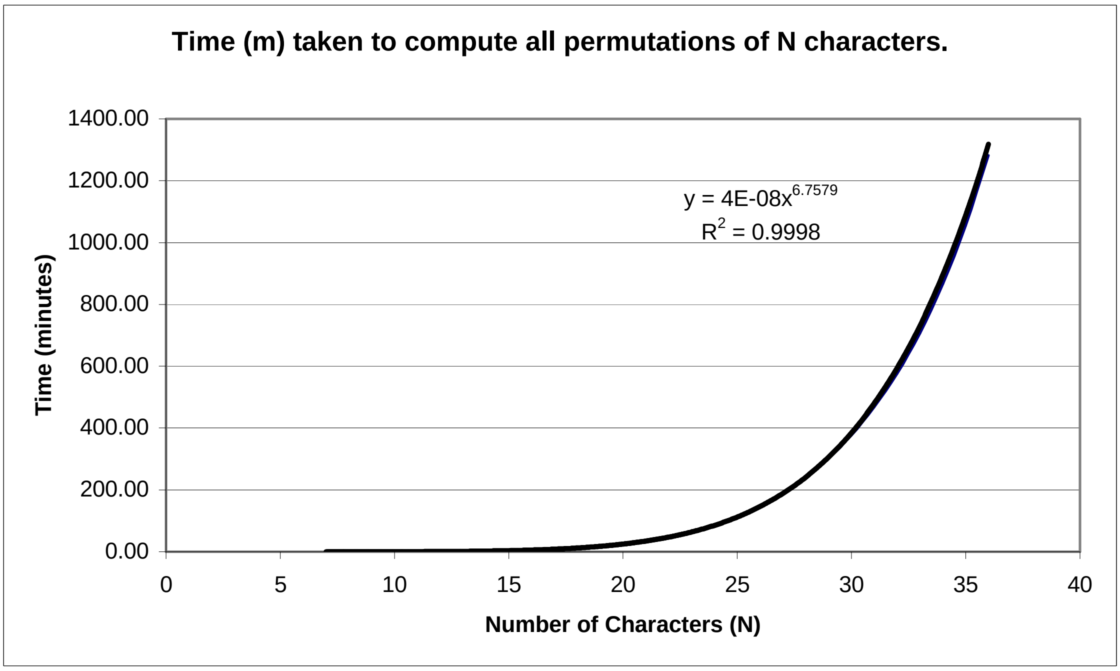


Figure 10: Time taken to compute all possible permutations of N characters***.***

As was shown in the “Theoretical statistic use” section, the expected amount of permutations the cracker program uses are given by.

$$1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7$$

It is possible to reduce it to a more simple equation. Multiply by (1-x)

$$(1-x)(1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7) = (1-x^8)$$

Therefore we can now write

$$1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 = (x^8-1)/(x-1)$$

This is a generic expression that holds for any value of x ($x \neq 1$). However, if x becomes much greater than one, then

$$x^8-1 \approx x^8$$

and

$$x-1 \approx x$$

and hence the expression further reduces to

$$1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 = (x^8-1)/(x-1) \approx x^8/x = x^7 \quad (x>>1)$$

Therefore for character sizes much greater than one(at least seven), one would expect the relationship between the number of characters (n) and the time (t) to follow the following relation equation:

$$t = k\,n^7$$

The constant k is dependant on the following:

- The specification of the computer used for the cracking (cpu size, memory size, type of processor etc.)
- The size of the password file that is being cracked
- The implementation of the cracking algorithm
- The speed at which passwords are cracked (If a lot of passwords are cracked early on, then there are less passwords to test, thus making the testing part of the algorithm much faster)

For a given configuration (cpu, memory, type of cracker used) it should be possible to compute the constant k. This will allow us to predict future times using the above equation.

It is possible to draw a graph of k by reversing the above equation and making k the subject of the equation:

$$k = t/n^7$$

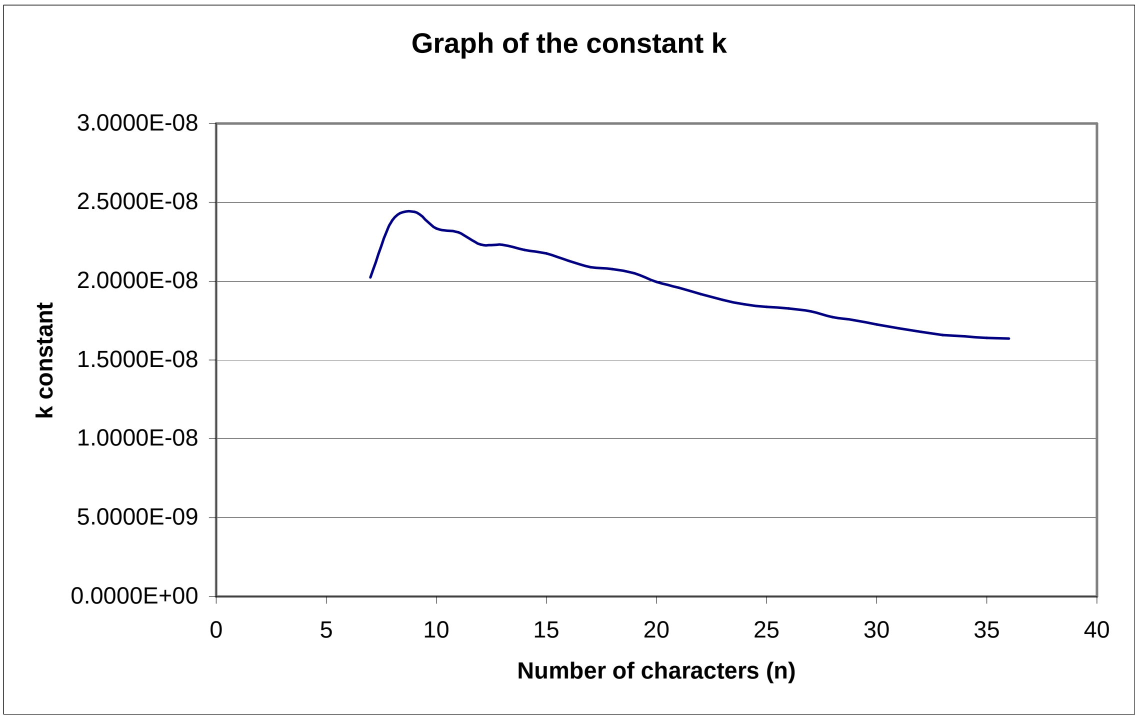


Figure 11: K constant as a function of the number of characters (n).

The graph above (Figure 11) shows that k is not constant as expected, but rather varies with n. This can be explained by the efficiency of the cracking algorithm. Thus the more letters used, the better the performance of the algorithm.

Thus k is the amount of time that the algorithm needs to test one single character combination against all the encrypted passwords that it wants to crack.

Therefore 1/k is the number of password-attempts that are being made per second. In this sense, 1/k is a direct measurement of the performance of the cracking algorithm, as well as the computer it is being executed on. Figure 12 shows 1/k, and that the algorithm is cracking more passwords per second for larger numbers of characters.

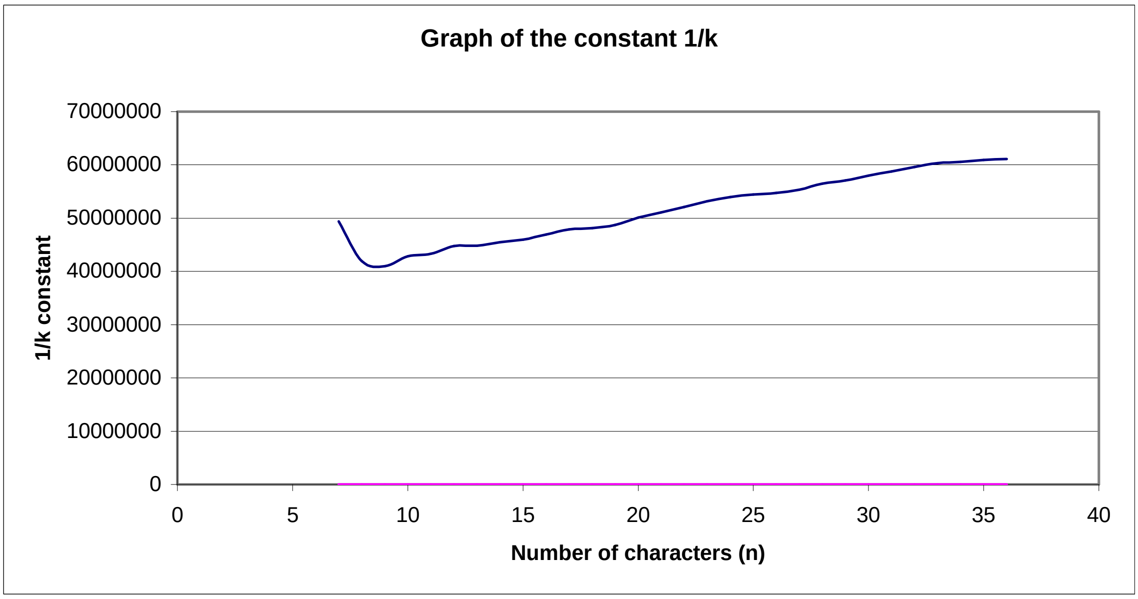


Figure 12: Experiment 1: Graph of the constant 1/k as a function of the number of characters (n**)**

The small “kink” at the start of both graphs may be explained by the fact that the time measurements for these experiments are very small, and thus more prone to error than that of the bigger character sets.

4.3.2 Character use Conclusion

The relationship between the number of characters and the time taken to crack these passwords was characterised. We found that this relationship follows can be demonstrated by a power relationship. By staging a theoretical attack on the problem it was shown that the relationship can be simplified to:

$$t = k\, n^{7}$$

The constant k is dependent on the hardware and software used to crack the passwords. For the configuration used to do these experiments this relationship becomes

$$t = 1.64x10^{-8} * x^{7}.$$

4.4 Password cracking

Character statistics can be used to optimise password cracking, The 46000 MySpace passwords were encrypted, and attacked by John the Ripper (Peslyak 2006).

4.4. 1 John the Ripper

John the Ripper is a password cracking tool originally developed for Unix, but has also been ported to use in the Windows operating system. After a password file has been obtained from a machine “John the Ripper” is used to crack the passwords within the password file. John has a number of options, including a specified character set.

For this study, the 46380 passwords were fist re-encrypted with the openssl command (OpenSSL 1999). OpenSSL is a cryptography toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) network protocols and related cryptography standards required by them.

By using the “openssl passwd” command, all of the 46380 passwords were re-encrypted with and new hashes generated. For example the password “ilovyou” hash can be calculated as follows:

```
openssl passwd ilovyou
```

The result of the above command was:

```
75zJEDdwuaPew
```

These hashes generated by “openssl passwd” is used by “John the Ripper” to calculate the original password. “John the Ripper” can be manipulated to use a predefined character set.

As a control, “John the Ripper” was tested on the full 46380 password hashes, and stopped after 16 hours. In this scenario “John the Ripper” was able to crack 3579 passwords. “John the Ripper” uses some of the following shortcuts to increase the search time per password hash:

- Lowercase every pure alphanumeric word
- Capitalize every pure alphanumeric word
- Lowercase and pluralize pure alphabetic words
- Lowercase pure alphabetic words and append '1'
- Capitalize pure alphabetic words and append '1'
- Duplicate reasonably short pure alphabetic words (fred -> fredfred)
- Lowercase and reverse pure alphabetic words
- Prefix pure alphabetic words with '1'
- Uppercase pure alphanumeric words
- Lowercase pure alphabetic words and append a digit or simple punctuation
- Words containing punctuation, which is then squeezed out, lowercase
- Words with vowels removed, lowercase
- Words containing whitespace, which is then squeezed out, lowercase
- Capitalize and duplicate short pure alphabetic words (fred -> FredFred)
- Capitalize and reverse pure alphabetic words (fred -> derF)
- Reverse and capitalize pure alphabetic words (fred -> Derf)
- Lowercase and reflect pure alphabetic words (fred -> fredderf)
- Uppercase the last letter of pure alphabetic words (fred -> freD)
- Prefix pure alphabetic words with '2' or '4'
- Capitalize pure alphabetic words and append a digit or simple punctuation
- Prefix pure alphabetic words with digits
- Capitalize and pluralize pure alphabetic words of reasonable length
- Lowercase/capitalize pure alphabetic words of reasonable length and convert:
- Crack -> cracked, crack -> cracking
- Try the second half of split passwords

The experiment calculated the number of passwords cracked with limited passwords sets. In Table 8, the number of passwords cracked in 32 hours with a limited character set is shown. The character set is also the set calculated in Table 5.

Table 8: Password cracking with limited characters

# Characters	**Cracked Passwords**
10	6
20	16
30	46
All letter and numbers (A-z,0-9)	30

4.4.2 Conclusion on Limited Character use

The number of passwords cracked is still significantly less than the number of passwords cracked through the “John the Ripper” default optimised mode. Thus, using the most frequent characters can reduce brute force search time, but is much less efficient than using a dictionary attack with character manipulations rules.

5 Conclusions

Password lists are available on the Internet. The use of the word “password” in Internet content has reached pandemic proportions, and complicates the search for password lists. Results from popular search engines such as Google are overwhelming. Superior results are obtained by using eMule. A significant password list, the 46 000 MySpace accounts password list, was obtained including full usernames.

Lists of default passwords used by hardware manufacturers can be obtained effortlessly. Thus the default passwords on new hardware should be changed immediately on commencing use. Even without a formal search, the default password for any hardware device can be guessed if the manufacturer is known. Popular default passwords are:

- admin
- password

From this and previous studies, the following passwords were ranked as the most popular:

- password
- 12345
- qwerty
- ilovyou
- letmein

By using only the characters that occur with a high frequency, the total brute force search time can be reduced significantly, but the resulting password cracking performance is not significantly better than when using all the letters and numbers in the set.

6 References

Brown S. (2006) “Top 10 Most Common Passwords”, [online] http://www.modernlifeisrubbish.co.uk/article/top-10-most-common-passwords

Geer, D. (2005), Chip makers turn to multicore processors, *IEEE Computer*

Golle, P. Leyton-Brown, K., Mironov, I. and Lillibridge M (2001), “Incentives for sharing in peer-to-peer networks”, Proceedings of the 3rd ACM conference on Electronic Commerce

Klein, D.V. (1990) *Foiling the Cracker: “*A Survey of, and Improvements to, Password Security*”*, *Proceedings of the United Kingdom Unix User's Group*, London

Morris, R. (1965) *Computation Center, CTSS Programmer's Guide, 2nd ed. Cambridge*, Mass.: M.I.T. Press,

Nielsen,*(2008) Nielsen NetRatings Search Engine Ratings*, http://searchenginewatch.com/showPage.html?page=2156451, Accessed 1June 2008

OpenSSL (1999), “OpenSSL man page” [online] http://www.openssl.org/docs/apps/openssl.html

PCMag, (2007), “10 Most Common Passwords” [online] http://www.pcmag.com/article2/0,1895,2113976,00.asp

Peslyak, A. (2006), “John the Ripper” [online] http://openwall.com

Ruska , J. (2008) “Most Common Passwords, “ [online] http://blog.jimmyr.com/Most_Common_Passwords_20_2008.php

van Heerden, R.P. Vorster, J.S. (2008) “Analysis of passwords”, *IFIP TC9 Proceedings on ICT uses in Warfare and the Safeguarding of Peace*, CSIR Pretoria South Africa

Wang, L. (1997) *“Hackers” Movie Script*, [online] http://www.freeinfosociety.com/site.php?postnum=402