

# Password Guidelines

Nigel Pentland

February 2001

## Introduction

The objective of this paper is to give some simple, easy to use guidelines on choosing passwords, particularly in relation to **Windows NT** and **IBM OS390 Security Server** (a.k.a. **RACF**).

Daniel V Klein [Klein1991] eloquently made the following points, which are just as true today as they were 10 years ago.

'Users are rarely, if ever, educated as to what are wise choices for passwords. If a password is in a dictionary, it is extremely vulnerable to being cracked, and users are simply not coached as to "safe" choices for passwords.'



'... many users also say "I don't care who reads my files, so I don't need a good password."

Regrettably, leaving an account vulnerable to attack is not the same thing as leaving files unprotected. In the latter case, all that is at risk is the data contained in the unprotected files, while in the former, the whole system is at risk.'

The problem of choosing good passwords goes way back to the earliest days of computing. The advent of better, faster computers only serves to aggravate this issue. A CERT<sup>1</sup> Incident Note [CERTIN-98.03] describes a compromised system found to contain details of 186,126 accounts of which 47,642 had been cracked, i.e. successfully guessed.

The SANS Institute publishes 'How To Eliminate The Ten Most Critical Internet Security Threats, The Experts' Consensus'<sup>2</sup>. Number 8 (Version 1.32 January 18, 2001) is described as 'User IDs, especially root/administrator with no passwords or weak passwords'.

The solution to this problem is simple, improve password quality.

Now that I have explained the issue, and hopefully generated some desire for users to improve their password quality, the following section goes on to give my rules of thumb for improving password quality. Then follows examples of bad passwords, and for those who want, detailed reasoning justifying each of the rules of thumb.

---

<sup>1</sup> CERT<sup>®</sup> Coordination Center, Carnegie Mellon University Software Engineering Institute

<sup>2</sup> SANS Institute Top Ten <http://www.sans.org/topten.htm>

## Rules of Thumb

# Rules

1. **Do not use the same password for Windows NT and RACF.**
2. **Always use a 7 character password for Windows NT**
3. **Do not use any ‘dictionary’<sup>3</sup> words (applies equally to Windows NT and RACF)**
4. **For Windows NT passwords always use at least one of the following characters**  
`[ ] \ ; ' , . / ~ ( ) { } | : " < > ?`
5. **Do not use numbers to create simple sequential passwords, especially on the right-hand end of the password**
6. **Where possible use unique random passwords, probably only practicable with the use of some form of ‘Password Safe’<sup>4</sup>**

## Bad Password Examples

A ‘bad’ password is quite simply one that has turned up in a password dictionary, or one that can be easily cracked. In Windows NT, anything containing only letters and numbers can be easily cracked (see rule 4 justified) !

Password	Comments
12345678	Simple keyboard pattern
Cocacola	Avoid brand names
Holidays	Variations of the word holiday or destinations are huge favourites
January	Dictionary word, also obvious sequence
LeedsUtd	Avoid team names, including UK football teams
Legin	Apart from being too short, it’s Nigel backwards
Lennon	Any name is bad, but especially well known ones
Password	The all time, ultimate, bad password
PissOff	Probably the ultimate emotive one, at least without getting obscene
Prelude	Avoid models of cars, etc.
R3dW1ngs	Dictionary words with simple numeric substitution
Sportscene	Avoid names of TV programmes
Sr1lanka	Place name with simple numeric substitution
Summer	So common you wouldn’t believe it
Uranus	Avoid names of planets, no matter how tempting

<sup>3</sup> This refers to the sort of dictionary used by hackers, i.e. lists of likely passwords such as peoples names, place names, dictionary words, etc.

<sup>4</sup> Password Safe is a public domain utility for securely storing User ID / Password pairs courtesy of Bruce Schneier and Counterpane <http://www.counterpane.com/passsafe.html>

## Justifications

1. The effort required to break a Windows NT password is significantly less than the effort required to break a RACF password. There are two primary reasons for this, namely:

First, the algorithm used to encrypt the passwords within Windows NT is much faster and hence it doesn't take as long to attack

Second, Windows NT is more prone to attack because if 2 users have the same password then they will each have the same encrypted password. This means that carrying out an attack on an entire Windows NT SAM<sup>5</sup> takes virtually the same length of time as attacking a single Windows NT user account. RACF on the other hand encrypts the password as a function of the user, and hence to attack 100 RACF user accounts takes 100 times longer than attacking just one.

2. Windows NT breaks the password into 7 character blocks and then encrypts each block separately. This means if you choose a 9 character password, it is in fact a 7 character password appended with a 2 character password. Cracking the last 2 characters is easy and often means giving a clue as to the first 7 characters.

Having a 14 character password, would equate to having two 7 character passwords and hence potentially stronger than one 7 character password. However, there is always a tendency for there to be some link between them, hence my advice to keep it simple, just stick with a 7 character password. If you do go for a 14 character password make sure you have a punctuation character in each of the 7 character blocks.

3. Dictionaries are one of the main forms of attack against computer systems. That is where an attacker simply automates trying possible passwords one after another. Note, in this context a dictionary is simply a list of possible passwords and they are likely to contain peoples names, place names, as well as likely substitutions, e.g. substituting the number one for the letter 'i' or the number zero for the letter 'o' etc..
4. The usual way to attack Windows NT passwords is first by a dictionary attack and then by a brute force attack. This is where every permutation of password is systematically tried one after another.

This is most commonly done with a program called L0phtcrack<sup>6</sup> which has 4 option settings for brute force attack. These options relate to the character sets used. Essentially to try every permutation can take a relatively long time, but if for example you can try every permutation of A-Z and 0-9 and obtain over 90% of all the passwords then it's like taking candy from a baby!

The 4 option settings for character sets are as follows:

```
A-Z
A-Z, 0-9
A-Z, 0-9, !@#$%^&*-_+=
A-Z, 0-9, -=[]\; ', . / ~ ! @ # $ % ^ & * ( ) _ + { } | : " < > ?
```

---

<sup>5</sup> SAM or Security Accounts Manager is the location within Windows NT of the list of valid user identities and encrypted passwords

<sup>6</sup> L0phtcrack is a cracking program written by L0pht Heavy Industries (a well known and highly competent hacking group) <http://www.securitysoftwaretech.com/l0phtcrack/download.html>

Hence my advice to use at least one character which is only found in the full blown option which takes a relatively long time to crack, i.e. one of the following:

[ ] \ ; ' , . / ^ ~ ( ) { } | : " < > ?

5. The majority of people when choosing passwords which expire periodically think of a password and append a number to it. This means that if the password gets comprised once, it can be easily guessed thereafter.
6. Using something like Password Safe is particularly useful for RACF passwords. However, beware that Password Safe is no different in as much as it too can become under attack. There is a Password Safe Cracker<sup>7</sup> openly available on the internet, hence the passwords held within Password Safe are only as secure as the initial password protecting the contents of the safe! Make sure the safe combination is not in a dictionary !!

## References

Klein1991.

Daniel V Klein, "Foiling the Cracker: A Survey of, and improvements to, Password Security"

CERTIN-98.03.

CERT Incident Note IN-98.03, "Password Cracking Activity"

---

<sup>7</sup> PasswordSafe Cracker by Joe Smith <http://members.aol.com/jpeschel3/PasswordSafeCracker.zip>