Password Facts & Fallacies

Simon Baker

simonb@sec-1.com

Topics

- Microsoft Password Quality Enforcement
- Password Cracking with Rainbow Tables
- Password Policy and Security
- Locking out Accounts
- Brute Force Attacks

Microsoft
Password Quality

Microsoft provide an on/off switch for password security!

“Password must meet complexity requirements”

Microsoft Password Quality

- *Must Be at least 6 Characters Long*
- *Must Contain a combination of 3 of the following :*

Uppercase Letters

Lowercase Letters

Numbers

Punctuation Marks

Microsoft Password Quality

The Documentation makes this rather exciting claim

"Passwords must meet complexity requirements to Enabled.

This policy setting, combined with a minimum password length of 8, ensures that there are at least 218,340,105,584,896 different possibilities for a single password.

This makes the use of a brute-force attack difficult, but still not impossible.

An attacker who had enough processing power to test 1 million passwords per second could determine such a password in about seven-and-a-half days or less."

Microsoft Password Quality

It’s a FAIL because...

Password1

will pass complexity checks....

Microsoft Password Quality

It’s a FAIL because...

- Changes are not applied retrospectively!
  - Users can choose whatever they like to begin with
  - Until they are forced to change their passwords, via setting or password ageing, weak passwords remain!

Microsoft Password Quality

It's a FAIL because...

- Service / Administrative accounts are almost always "never have to change password"
- All too often Domain Admin accounts are created unnecessarily for services
- A lot of the time the password /is/ the username

Microsoft Password Quality

- Hard not to bash Microsoft, though they're not alone in all this!
- Most other OS' have had similar failings as well...
- However, Microsoft did bring us the wonderous LANMAN hash!
- Which leads us nicely onto...

Rainbow Tables Overview

Rainbow Tables are...

- "a code book for a hash function"
- "a lookup table designed to help recover plaintext from a one-way hash"

This is known as a time-memory trade off because it consumes enormous time to create, but once they are created password recovery is -very- quick.

Rainbow Tables

- In essence, you pre-compute the hashes from plain text

- You then look up the hash of the plain text

The above is not actually true, and this URL explains why

http://kestas.kuliukas.com/RainbowTables/

Rainbow Tables

- How big are they?
- How fast are they?
- How “good” are they?

Real World Passwords

Selected Sites

Universities

Local Government

NHS Primary Care Trusts

Windows Hashes

Selected sites still running LANMAN

Site A – Cracked 11489 / 11958 (96%) in 5 hours

Site B – Cracked 5232/5756 (91%) in 5 hours

Site C – Cracked 3186/3561 (89%) in 5 ½ hours

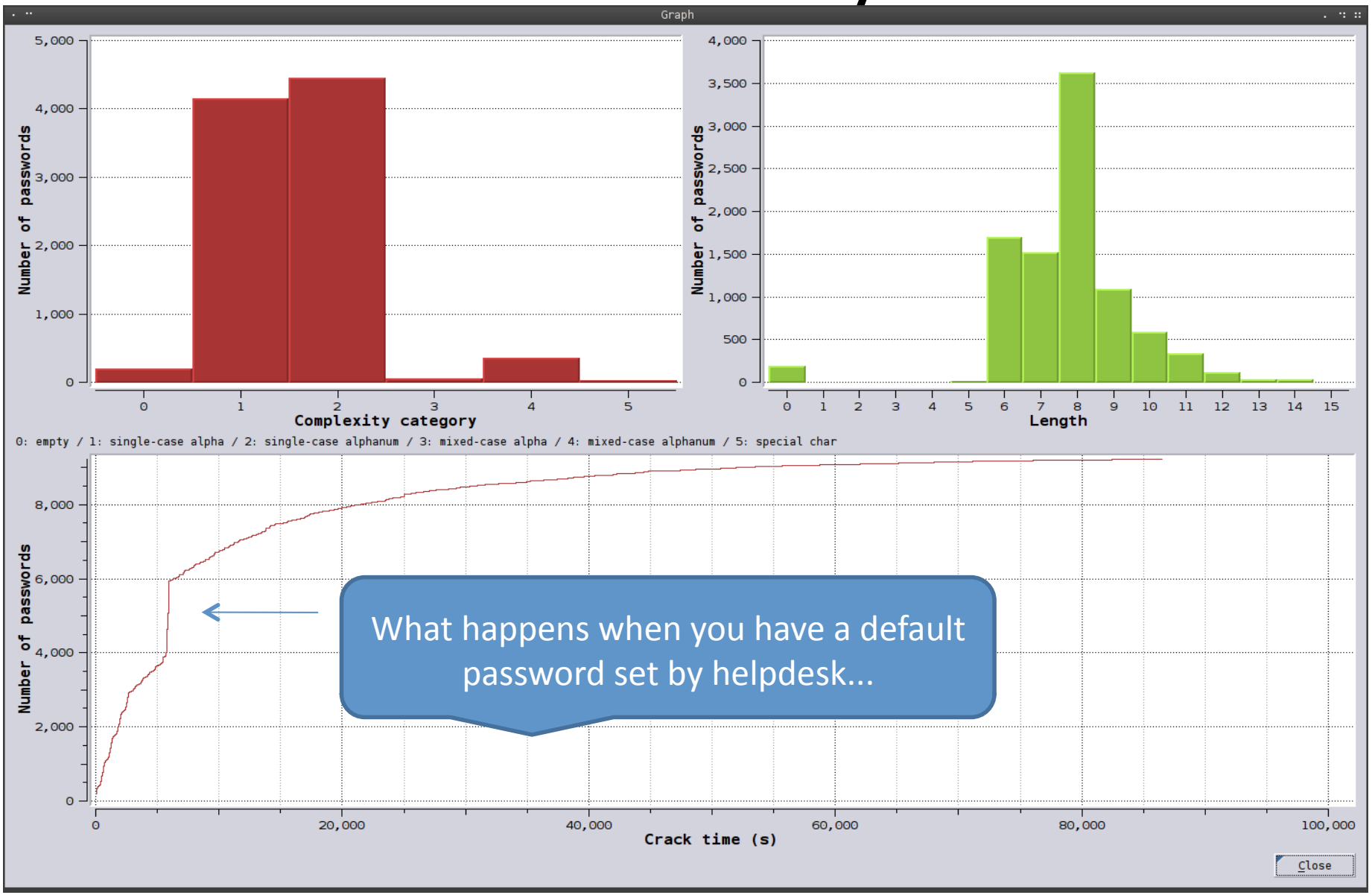
Site D – Cracked 1184/1287 (95%) in 1 Hour

Site E – Cracked 9224/14293 (65%) in 24 hours (!)

Site F – Cracked 936/2063 (45%) in 10 hours (!)

Site G – Cracked 6243/6861(91%) in 6 hours

Site E - Analysis



Rainbow Tables

- Of course, you need to already have the password hashes to do this...
  - Chicken and Egg
- So, how do you get the hashes?
  - Need to be a Domain Admin on a DC
  - How do we get to Domain Admin?
    - Either by exploiting something or
    - By Brute Force....

Lockout Timeouts

What is the "Locked account time" Setting?

- It's the time an account will be "locked" for when the following two conditions are met:

Time between failed logon (s)

Number of invalid logon before locked out (s)

Lockout Timeouts

Example Settings

Locked account time (s) 900

Time between failed logon (s) 900

Number of invalid logon before locked out (s) 3

If Fred types his password wrongly 3 times in 15 minutes, he will be unable to try to enter it again for 15 minutes.

Lockout Timeouts

Insanity Ensues

- Why does that increase security?
  - I don't think it does...
- The only purpose that seems to serve, is to irritate:
  - It irritates Fred, who by now is on the phone
  - It irritates Helpdesk, who are coincidentally also on the phone...

Lockout Timeouts

- At most clients, I normally see lockout times of between 900 and 1800 seconds (15 mins, 30 mins).
- I once saw a site had a lockout policy of 120 seconds
- I was going to report it as an issue, that it needed increasing, but then I had a think about it....

Lockout Timeouts

What I'd Recommend (*)...

Locked account time (s) 60

Time between failed logon (s) 60

Number of invalid logon before locked out 3

WHY?

** I'm certain your auditor will disagree ☹*

Lockout Timeouts

- Fred would need to type his password once every 20 seconds to hit the limit ;
  - Most humans tend to stop and think ...
  - "*Was* that the right password...? Did I *missslep it*?"
- If fred does lock out his account, he only has to wait a minute ;
  - With education, Fred knows he just needs to pop the kettle on and try again...

Lockout Timeouts

- With setting of 3 passwords, and a lockout of 60 seconds, a brute force attack would be able to try....

180 passwords an hour?

Not going to be very fruitful!

(or is it..?)

Brute Forcing Accounts

- It’s very quick to brute force accounts
- No tool I’ve ever used has a rate of trying 3 passwords in 15 minutes
- Orders of magnitude faster, thc-hydra 16,500 passwords tried in ~1 minute

But why try one username and 1000 passwords, when you can try one password and a 1000 usernames ? ;-)

Confessions of A Pentester

Or "*How to Smash in an Account*"

- Brute Force Attacks really do Work!
- Try the following attacks and ...
- *...it will be fruitful...*

Confessions of A Pentester

- Enumerate Users on the Domain
- Enumerate Password Lockout Policy
- Perform an attack, with a minimal set of passwords – assuming a 3 strikes policy....

Password = username

Password = password

Password = blank

Does that Really work?

- Site A – 234 users had a password “password”
- Site B – 13 users ....
- Site C – 0 users (!) ....
- Site D – 363 users ....
- Site E – 2108 users (one in 6....)
- Site F – 1 user ....
- Site G – 207 users ....

One Month Password Change

- Where did this come from?
  Gene Spafford believes:
  - From back in the days when people used non-network mainframes
  - CPU time was expensive
  - Some DoD contractors did some back-of-the-envelope calculations
  - This was then enshrined in policy, which got published, and largely accepted by others over the years.

Password Aging

Chris Roberts / Imperial College, London via *uk-security* asked....

"If you find any good research on correlation of short password expiry age and poor password practices, I'd love to know. We discussed this many times with the auditors - enforcing a short password expiry period results in people choosing systematic passwords (Chrisis1, Chrisis2) etc... "

Well, just quickly then...

los_stupidos_history_0:2272:EE386F96648290CA0EB6B32EF8DBE011:8
A:WEDNESD:AY8:wednesday8

los_stupidos_history_1:2272:EE386F96648290CA283D6D670F95A0C9:5
6:WEDNESD:AY7:wednesday7

los_stupidos_history_2:2272:EE386F96648290CAE4854A1029E103A4:3
E:WEDNESD:AY6:wednesday6

los_stupidos_history_3:2272:EE386F96648290CA2B4D67C72B9F2294:6F9185D00048BC892D8DB97A46F5080
0:WEDNESD:AY5:wednesday5

los_stupidos_history_4:2272:EE386F96648290CA8C7D9A51080ADB95:2BE8EB262B2AEFF71226ECC56DDF830
4:WEDNESD:AY4:wednesday4

los_stupidos_history_5:2272:EE386F96648290CACB85299E800060B9:3ABDBF9B0366C4008631259AE8D4C6D
C:WEDNESD:AY3:wednesday3

los_stupidos_history_6:2272:EE386F96648290CABE21A9B8F76DDE25:6F90E6092FD2795863CBBB69FCC82B3
0:WEDNESD:AY2:wednesday2

los_stupidos_history_7:2272:EE386F96648290CA431BB32CD5045E53:BCD59A6AECB5CF04022872CCFA9EA98
7:WEDNESD:AY1:wednesday1

los_stupidos_history_8:2272:EE386F96648290CAB9758222A30C3716:9FACDA6EE4470EB5C7A11983D46AE84
2:WEDNESD:AY:wednesday

los_stupidos_history_9:2272:0FBFC0DB42F4E67CB79AE2610DD89D4C:
6C0FCCC93B20BD884B6F1B4161563581:SATURDA:Y:saturday

los_stupidos_history_10:2272:AE5C85416D667EBEB79AE2610DD89D4C:
88A700C2AA250BE671EA7F9BC16B219B:THURSDA:Y:Thursday

los_stupidos_history_11:2272:E52CAC67419A9A224A3B108F3FA6CB6D:
8846F7EAEE8FB117AD06BDD830B7586C:PASSWOR:D:password

los_stupidos_history_12:2272:DDBF5909B25C75EF06F96CC9A50B276D:ACB00DD8715EA5E941D999ECB3F3B
867:::

- los_stupidos_history_0:2431:60BC03D561EB1E2A1AA818381E4E2
785A0FE15CE6F361CAD3E88D9E4E9E3A:SILVER2:3:silver23
- los_stupidos_history_1:2431:60BC03D561EB1E2A1D71060D896B7
639EF:SILVER2:2:silver22
- los_stupidos_history_2:2431:60BC03D561EB1E2AC2265B23734E0
5D8756409391A5BCD03D0C98C10A102B:SILVER2:1:silver21
- los_stupidos_history_3:2431:60BC03D561EB1E2A25AD3B83FA6627C7:F6F5080690CAF89A3F7237F57E4
A770E:SILVER2:0:silver20
- los_stupidos_history_4:2431:7DC59D4C59FFEFF409752A3293831D17:2FB5490E3FD2A8030D8E93277A6
333FD:SILVER1:9:silver19
- los_stupidos_history_5:2431:7DC59D4C59FFEFF436077A718CCDF409:D533E29FA09B746677414C3AD51
2073B:SILVER1:8:silver18
- los_stupidos_history_6:2431:7DC59D4C59FFEFF47C3113B4A1A5E3A0:F745D321780F9EF624B14F5D5DB
8F3BA:SILVER1:7:silver17
- los_stupidos_history_7:2431:7DC59D4C59FFEFF4C81667E9D738C5D9:E48A9180949C9828DB01BB831D
EBEF6:SILVER1:6:silver16
- los_stupidos_history_8:2431:7DC59D4C59FFEFF49C5014AE4718A7EE:
0122CE4C78284E8B885124958991FBAF:SILVER1:5:silver15
- los_stupidos_history_9:2431:7DC59D4C59FFEFF4FF17365FAF1FFE89:3475AD8806A7802E166647F343F1
983B:SILVER1:4:silver14
- los_stupidos_history_10:2431:7DC59D4C59FFEFF41AA818381E4E281B:DFA43EBE58BA8C6B67D3CBF343
1F5A05:SILVER1:3:silver13
- los_stupidos_history_11:2431:DDBF5909B25C75EF06F96CC9A50B276D:ACB00DD8715EA5E941D999ECB
3F3B867:::

Password Aging

- I’m going to keep quiet....
- I can see arguments both for and against...
- I still maintain however, if passwords are strong enough in the first place...

Final Thoughts...

Choose a Good Password

Choosing a Good Password

- Special characters
  - Always use a special character in your administrative passwords
  - I don't mean ¬*!"£$%^&*()*.....
  - I mean ôĂű...
- How do you generate those?
  - On a laptop, generally Fn+NumLk then ALT+ numbers on the keypad.
  - Use > 128 and < 256

People first, Technology second