

No More Passwords!



Mikael Simovits – 20091104

Where are passwords used?

- ❑ OS-authentication
 - Windows, Linux, UNIX etc
- ❑ Network authentication
 - NTLMv1, NTLMv2, LanMan, WPA2-PSK etc.
- ❑ Protecting encryption keys
 - PGP, Filebased certificates with private key etc. (National Certificates)

How are passwords protected?

- ❑ Encrypted
 - ❑ 3DES, AES....
- ❑ Timedelays introduced in verifying passwords.
 - ❑ DES repeated 20000 times....
- ❑ Demand increasing lengths
 - ❑ >8 char
- ❑ Demand increasing complexity
 - ❑ A...Ö + a...ö + 0...9 + !"#\$%&'()*=?+

Additional problems

- ❑ Password guessing techniques
 - Most probable password is guessed first
 - Word, Word+1-3digits,random
 - Rainbow tables – precomputed tables
 - Only non-salted passwords
 - GPUs are cheap
 - Some solutions have built in delays and some not.
 - NTLM: 160 million guesses/second
 - WPA-PSK: 60 000 guesses/second
 - NationalID: 16 000 guesses/second
 - Trojan sniffers are cheaper and simpler

Attacks

Stage 1

- Sniffing encrypted passwords
- Stealing password files with hashes
- Trojan keyboard sniffer

Stage 2

- wordlist guessing
- Brute Force (all passwords)
- Rainbow tables (non salted password)
 - LM, MD5, NTLMv1

Password Cracking Techniques

Type	Description	Speed (guesses/sec)
100 MHz	Simple 100 MHz PC	1 million
PC	Ordinary home PC 2009	10 million
WS	High perf. Work station 2009	150 million
Dual GPU	PC with Dual GPU 15000 SEK	1.6 billion
Rainbow GPU	PC with one GPU and Rainbowcrack 1.4	103 billion

Password Cracking Speed

A...Ö		Random – 29 characters			
#Char	<i>100 Mhz</i>	<i>PC 2009</i>	<i>WS 2009</i>	<i>2GPU</i>	<i>Rainbow + GPU</i>
8	6 d	14 h	1 h	5 min	5 sec
9	24 w	2 w	1 d	3 h	2 min
10	13 y	70 w	5 w	3 d	1 h

Password Cracking Speed

A...Ö,a...ö, 0-9		Random – 68 characters			
#Char	<i>100 Mhz</i>	<i>PC 2009</i>	<i>WS 2009</i>	<i>2GPU</i>	<i>Rainbow + GPU</i>
8	15 y	1 y	5 w	3 h	1 h
9			3 y	32 w	4 d
10				42 y	35 w

Password Cracking Speed

A...Ö,a...ö, 0-9,!\"#...(		Random – 102 characters			
#Char	<i>100 Mhz</i>	<i>PC 2009</i>	<i>WS 2009</i>	<i>2GPU</i>	<i>Rainbow + GPU</i>
8				12 w	1 d
9				24 y	20 w

Min password requirements 2009

- ❑ Password must be random
 - At least one char a...ö
 - At least one char A...Ö
 - At least one char 0...9
 - At least one char !"#\$%&'()*+,-./:;<=>?@[\]^_`{|}~
- ❑ Minimum 10 characters (not salted)
- ❑ Minimum 9 characters (salted)
 - Example:
 - !Beer4Me2
 - ()Aq234T!

Why passwords will not work.

