

# Assless Chaps: a novel combination of prior work to crack MSCHAPv2, fast

(or why MSCHAPv2 doesn't cover it's ass)

by Michael Kruger @\_cablethief  
& Dominic White @singe

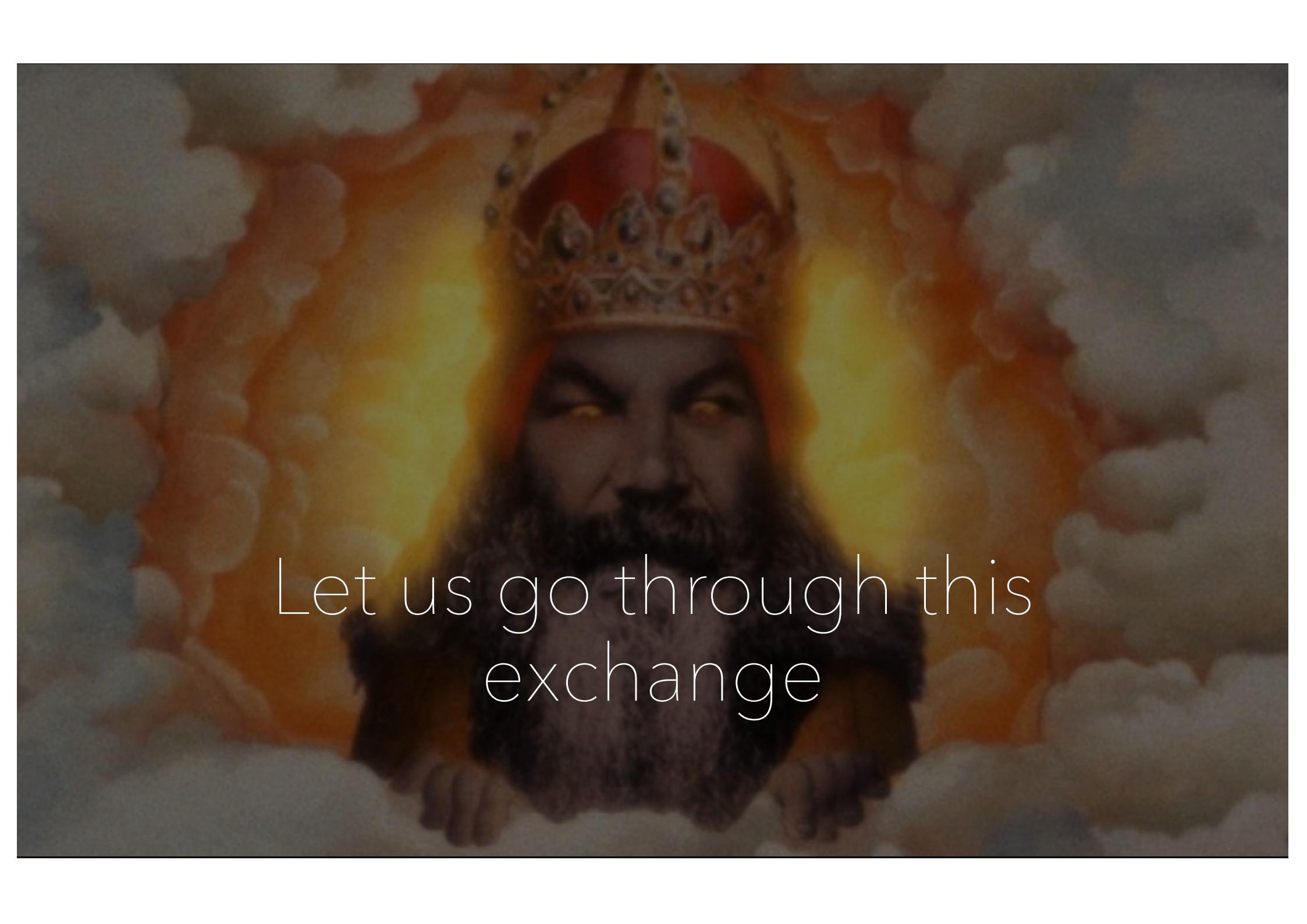
Orange Cyberdefense's SensePost Team

*industry*

hackers

MSCHAPv2

No, that's not dead.  
It's resting.



Let us go through this  
exchange



username

I am King Arthur



authenticator challenge

I challenge you!



peer challenge

I challenge you back!



NT response

I??;S???^?پQ?e4L??

Challenge = ChallengeHash(PeerChallenge, AuthenticatorChallenge, UserName)  
NTResponse = ChallengeResponse(Challenge, PasswordHash)



My swallow knowledge is  
beyond reproach!



authenticator response

,`Pչ<C{ 'K寫^pu6

AuthenticatorResponse = GenerateAuthenticatorResponse(PasswordHashHash,  
ChallengeHash, NTResponse)  
Success (S=)

F





# Challenge Generation

SHA

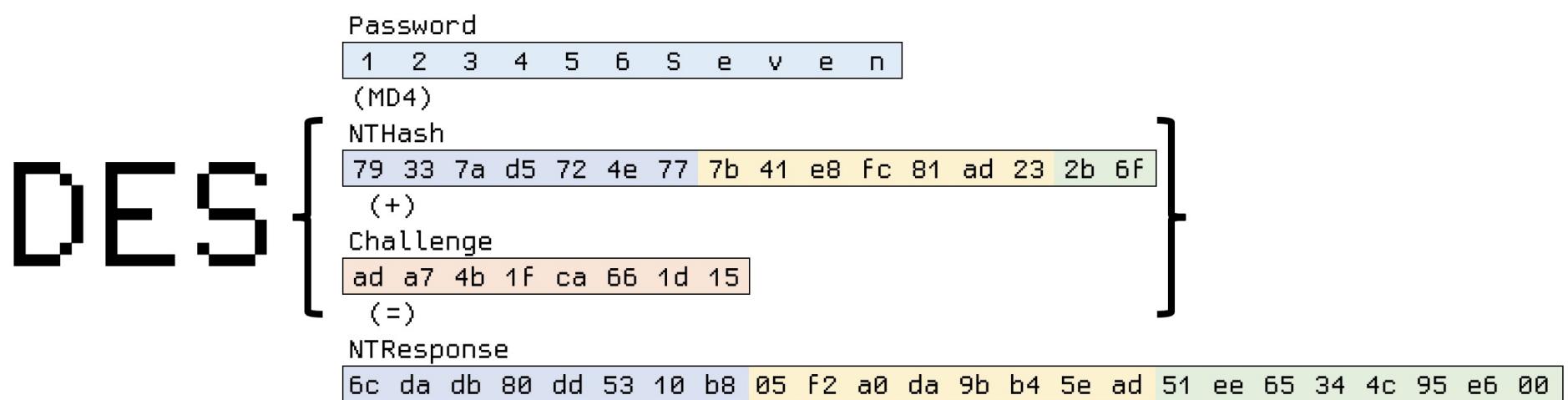
Username  
O l i v e r . P a r k e r  
(+)

AuthenticatorChallenge  
F5 b8 ad ee e9 FF 08 15 dd 83 e8 2d 89 6e eb 2a  
(+)

PeerChallenge  
e3 32 bf 8e c5 37 e5 72 1d 0d 9a 0e e4 40 46 d6  
(=)

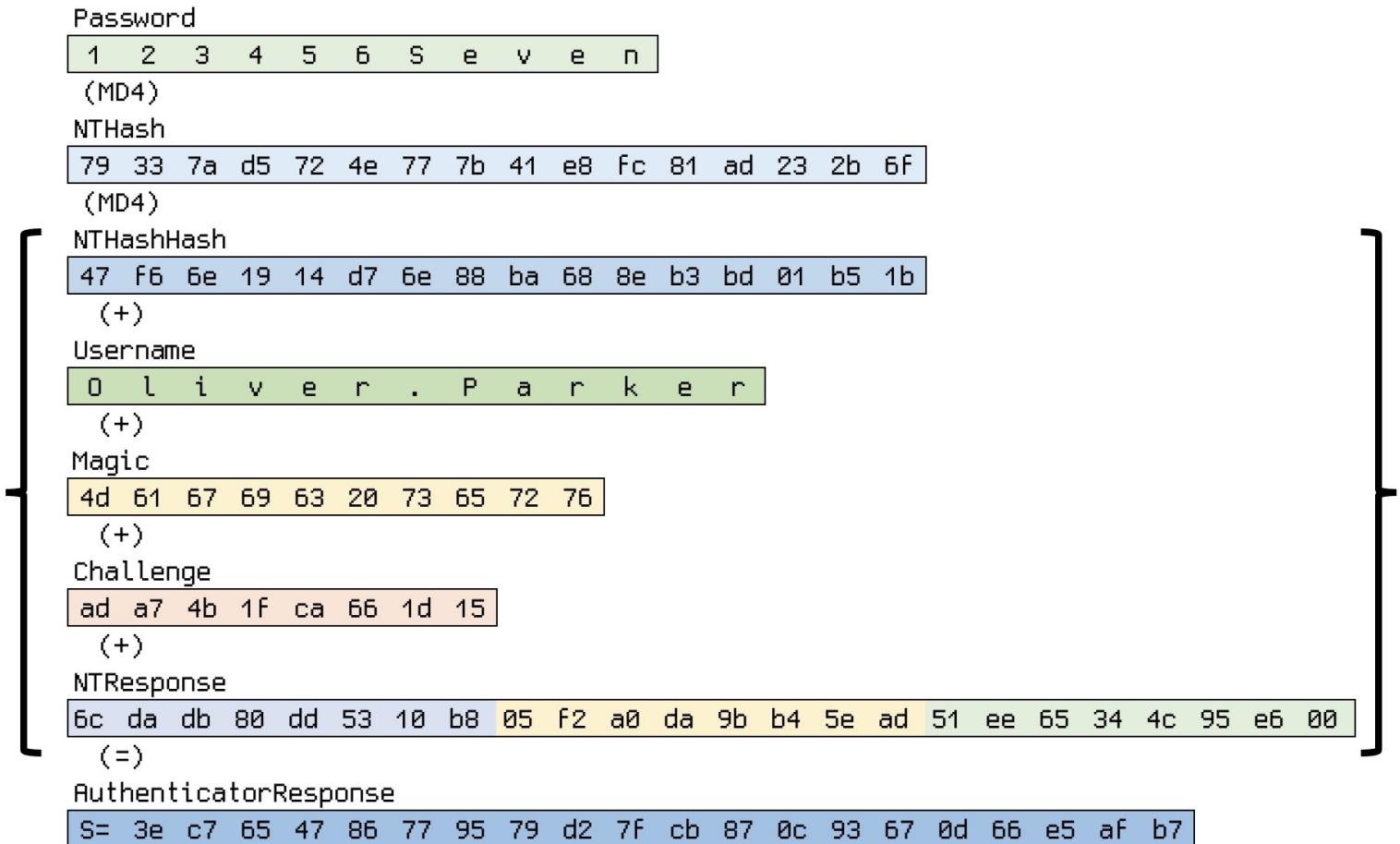
Challenge[0:8]  
ad a7 4b 1f ca 66 1d 15

# NTResponse Generation



# AuthenticationResponse Generation

SHA



# NTResponse Generation

DES {

    Password

    1 2 3 4 5 6 S e v e n

    (MD4)

    NTHash

    79 33 7a d5 72 4e 77 7b 41 e8 fc 81 ad 23 2b 6f

    (+)

    Challenge

    ad a7 4b 1f ca 66 1d 15

    (=)

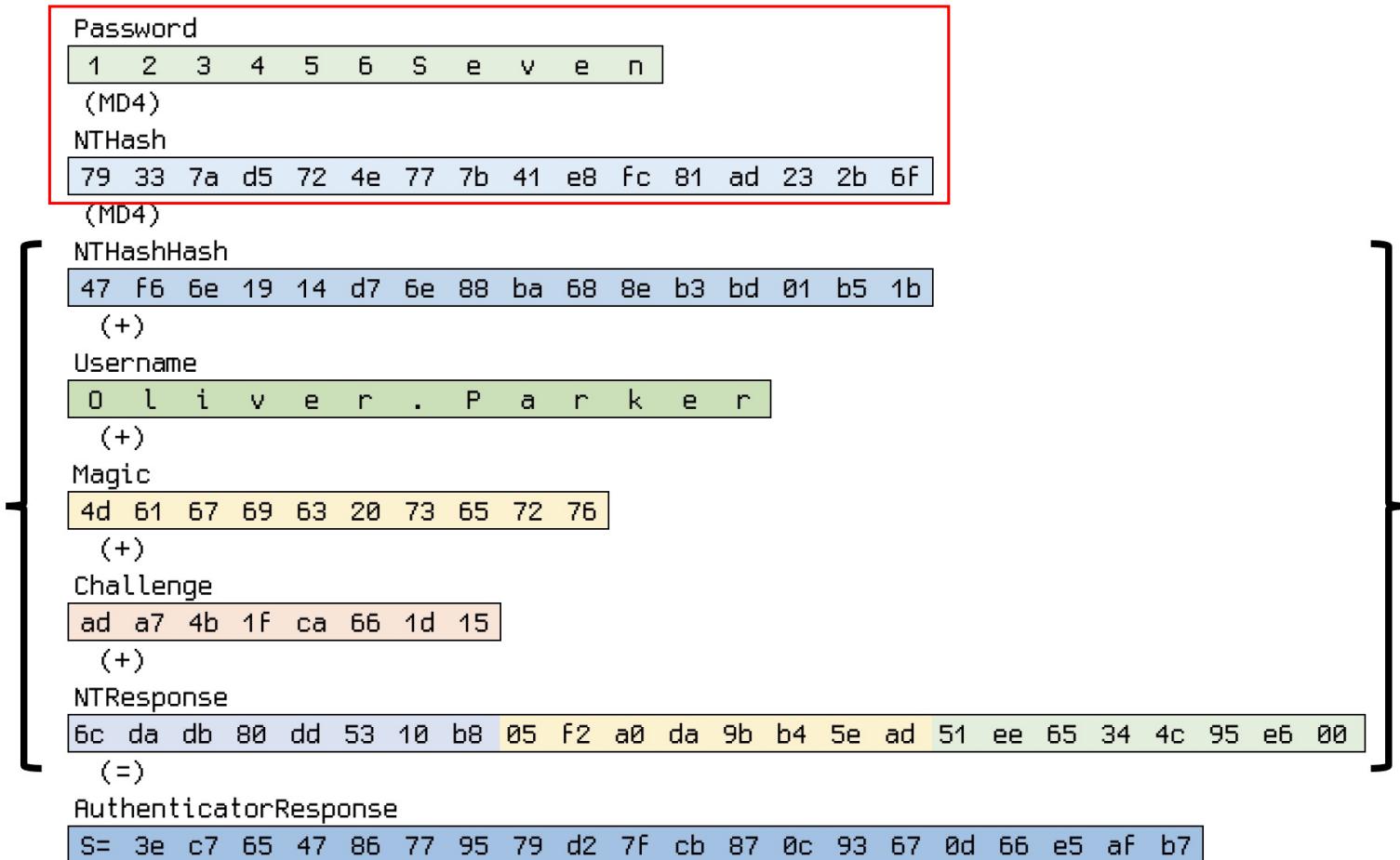
    NTResponse

    6c da db 80 dd 53 10 b8 05 f2 a0 da 9b b4 5e ad 51 ee 65 34 4c 95 e6 00

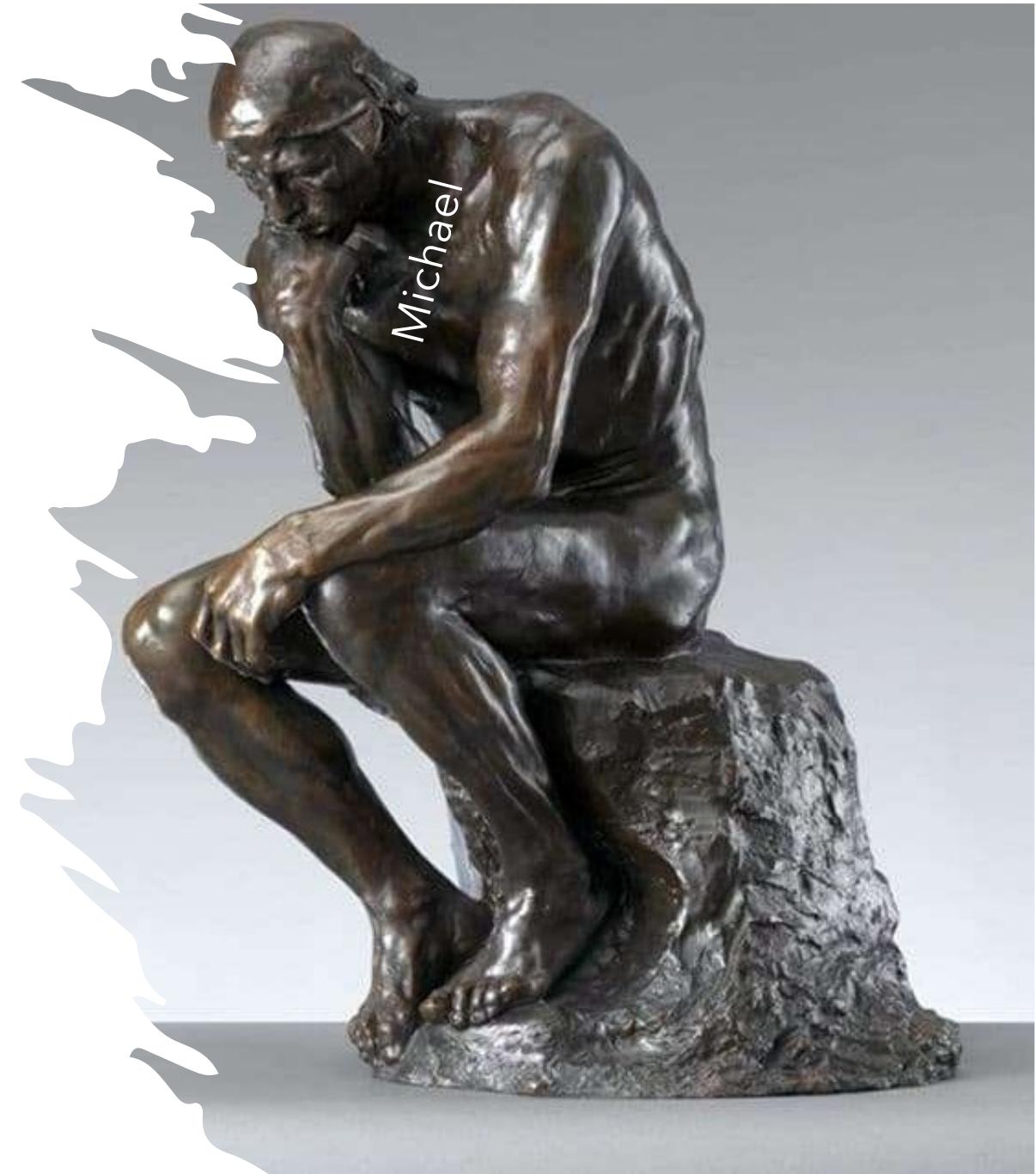
}

# AuthenticationResponse Generation

SHA



MSCHAPv2  
hmmmmm...



A close-up portrait of Mr. Spock from Star Trek. He has his signature dark brown hair in a flat-top style and a full, reddish-brown beard and mustache. He is wearing a blue Starfleet uniform with a visible collar. The background is dark and out of focus.

NT Hash

A close-up portrait of Mr. Spock from Star Trek, looking directly at the viewer with a serious expression. He has his characteristic pointed Vulcan ears and a small goatee. He is wearing a dark blue shirt. A single lit cigarette is held between his fingers, with a plume of blue smoke rising from it. The background is dark and out of focus.

Pass the Hash

# hostapd & wpa\_supplicant support it

```
network={  
    ssid="example"  
    scan_ssids=1  
    key_mgmt=WPA-EAP  
    eap=PEAP  
    identity="Oliver.Parker"  
    password="hash:79337ad5724e777b41e8Fc81ad232b6F"  
    ca_cert="/etc/cert/ca.pem"  
    phase1="peaplabel=0"  
    phase2="auth=MSCHAPV2"  
}
```

```
# Phase 1  
*      PEAP  
  
# Phase 2 (tunneled within EAP-PEAP or EAP-TTLS) users  
"Oliver.Parker" MSCHAPV2 hash:79337ad5724e777b41e8Fc81ad232b6F [2]
```

# Hashlists instead of Wordlists

- Current MSCHAPv2 modes take long
- There are a lot of wasted NThashes if you only use cracked ones
- There are places you can get NT hashes
  - Have I been Pwned, Active Directory, etc

## Pwned Passwords

Pwned Passwords are 613,584,246 real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. [Read more about how HIBP protects the privacy of searched passwords.](#)

# Hashcat Forums 2016

## How to make use of the DES KPA mode



09-03-2016, 11:39 AM

Just wanted to make a quick writeup how to use the new DES

An interessting example, I thought, would be how to retrieve from the server to enforce some challenge or if you sniffed it from t

## Reversing MSCHAPv2 to NTLM



10-01-2016, 03:46 AM (This post was last modified: 10-02-2016, 03:40)

So as we all know mode 14000 generic DES can be used for promised. This demo used \$99 format which is MSCHAPv2 here <http://markgamache.blogspot.ca/2013/01/n...roken.html>

# My New Hashcat Modes

5500		NetNTLMv1	/	NetNTLMv1+ESS
27000		NetNTLMv1	/	NetNTLMv1+ESS (NT)
5600		NetNTLMv2		
27100		NetNTLMv2	(NT)	

# New Hashcat Modes Demo

Part of hashcat main branch as of 3 Aug 2021 (thanks atom)

# A new approach

Let's talk about the ~~arse~~ ass

# MSCHAPv2 NT Response DES Encryption

Password Hash 79 33 7a d5 72 4e 77 7b 41 e8 fc 81 ad 23 2b 6f

# MSCHAPv2 NT Response DES Encryption

Password Hash	79 33 7a d5 72 4e 77 7b 41 e8 fc 81 ad 23 2b 6f
Key 1	79 33 7a d5 72 4e 77
Key 2	7b 41 e8 fc 81 ad 23
Key 3	2b 6f

# MSCHAPv2 NT Response DES Encryption

Password Hash    

79	33	7a	d5	72	4e	77	7b	41	e8	fc	81	ad	23	2b	6f
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

Key 1    

79	33	7a	d5	72	4e	77
----	----	----	----	----	----	----

Key 2    

7b	41	e8	fc	81	ad	23
----	----	----	----	----	----	----

Key 3    

2b	6f	00	00	00	00	00
----	----	----	----	----	----	----

padding

# MSCHAPv2 NT Response DES Encryption

Password Hash    

79	33	7a	d5	72	4e	77	7b	41	e8	fc	81	ad	23	2b	6f
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

Key 1    

79	33	7a	d5	72	4e	77
----	----	----	----	----	----	----

Key 2    

7b	41	e8	fc	81	ad	23
----	----	----	----	----	----	----

Challenge

ad	a7	4b	1f	ca	66	1d	15
----	----	----	----	----	----	----	----

Key 3    

2b	6f	00	00	00	00	00
----	----	----	----	----	----	----

padding

NTResponse    

6c	da	db	80	dd	53	10	b8	05	f2	a0	da	9b	6v	5e	ad	51	ee	65	34	4c	95	e6	00
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

# MSCHAPv2 Cryptanalysis

Challenge ad a7 4b 1F ca 66 1d 15

NTResponse 6c da db 80 dd 53 10 b8 05 f2 a0 da 9b 6v 5e ad 51 ee 65 34 4c 95 e6 00

# MSCHAPv2 Cryptanalysis

# MSCHAPv2 Cryptanalysis - The Ass

Key3 2b 6f 00 00 00 00 00 ass	(+) Challenge (=) padding	Ciphertext3 51 ee 65 34 4c 95 e6 00
-------------------------------------	------------------------------	--

## Password Hash

# Keyspace

0x0000 - 0xFFFF

0 - 65535

Joshua Wright  
DC11 2003

## MS-CHAPv2 Weaknesses

- MS-CHAPv2 weaknesses apply to the LEAP exchange
  - No salt in stored NT hashes
    - Permits pre-computed dictionary attacks
  - Weak DES key selection for challenge/response
    - Permits recovery of 2 bytes of the NT hash
  - Username sent in clear-text
  - We can deduce authentication passwords



# Moxie Marlinspike & David Hulton

## DC20 2012



Defeating PPTP VPNs and WPA2 with CHAPv2

An MS-CHAPv2 attack with a 100% success rate

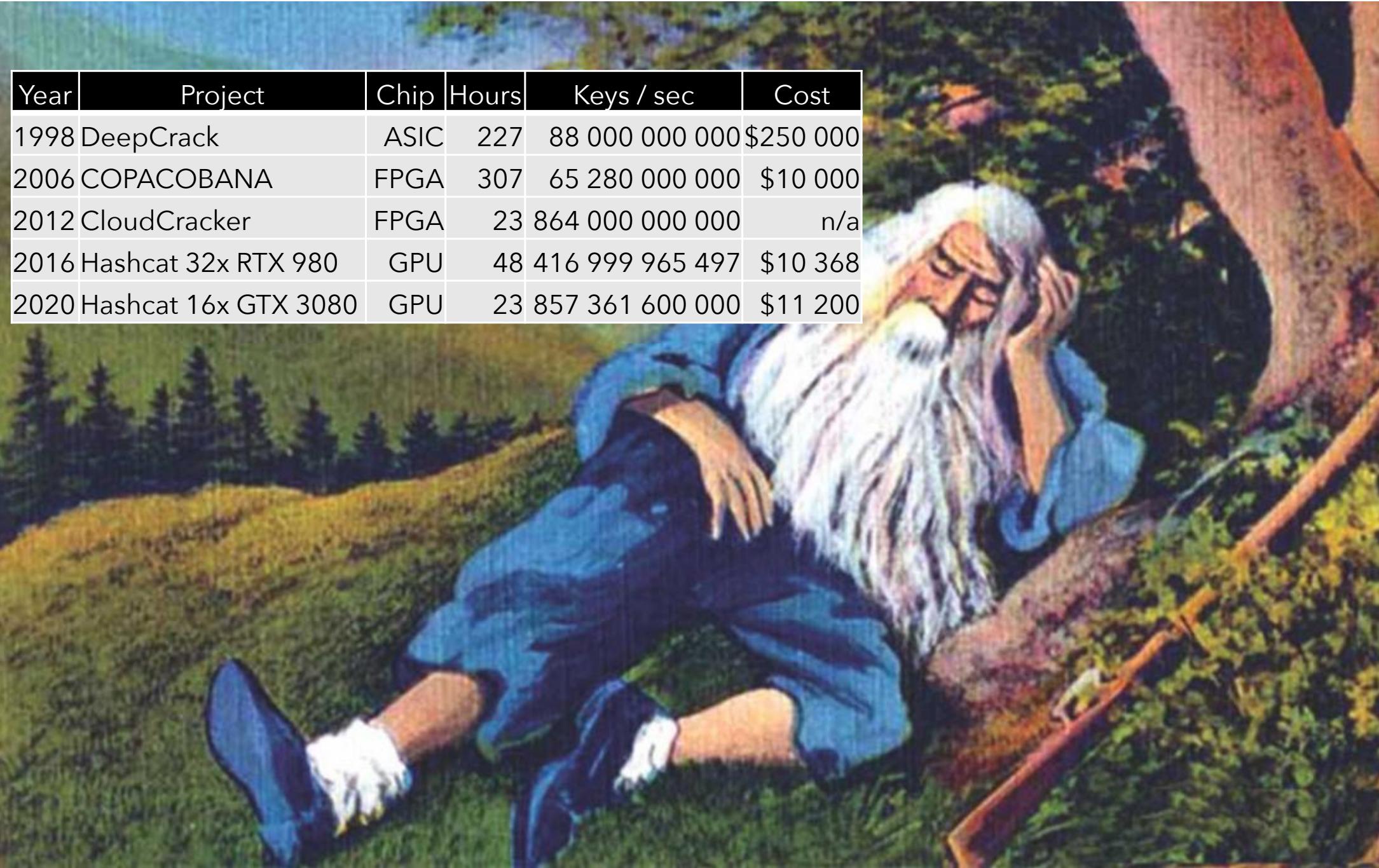
# MSCHAPv2 Cryptanalysis

## Single DES Round

Reduce two DES rounds to one - Encrypt once, compare twice  
 $2^{56}$  is 7 bytes aka 72 057 594 037 927 935

For i in 0 to  $2^{56}$

```
result = DEScrypt(cleartext=challenge, key=i)
if result == ciphertext1: key1 = i
if result == ciphertext2: key2 = i
```



Year	Project	Chip	Hours	Keys / sec	Cost
1998	DeepCrack	ASIC	227	88 000 000 000	\$250 000
2006	COPACOBANA	FPGA	307	65 280 000 000	\$10 000
2012	CloudCracker	FPGA	23	864 000 000 000	n/a
2016	Hashcat 32x RTX 980	GPU	48	416 999 965 497	\$10 368
2020	Hashcat 16x GTX 3080	GPU	23	857 361 600 000	\$11 200

# MSCHAPv2 doesn't protect its ass

Key3		Ciphertext3
<code>2b 6f 00 00 00 00 00</code>	(+) Challenge (=)	<code>51 ee 65 34 4c 95 e6 00</code>
ass	padding	

## Password Hash

```
grep 2b6F$ NTLM-hashlist.txt
```

# Initial (worst) Performance

<b>hash</b>	<b>tool</b>	<b>small</b>	<b>HIBP</b>
hash1	hashcat	8.778s (2250.6 kH/s)	2:58.84 (5662.4 kH/s)
	assless	0.860s	46.393s
hash2	hashcat	9.627s (1985.2 kH/s)	1:04.39 (5241.2 kH/s)
	assless	0.696s	41.152s



Bravely bold Sir Robin  
Rode forth from Camelot

A photograph of a dark, narrow path through a dense forest. The path is covered in fallen leaves and branches. Several pieces of white text are overlaid on the image, appearing as if they are floating in the air.

# The Dark Path of Perf Optimisation

ripgrep

indexes!

file tricks

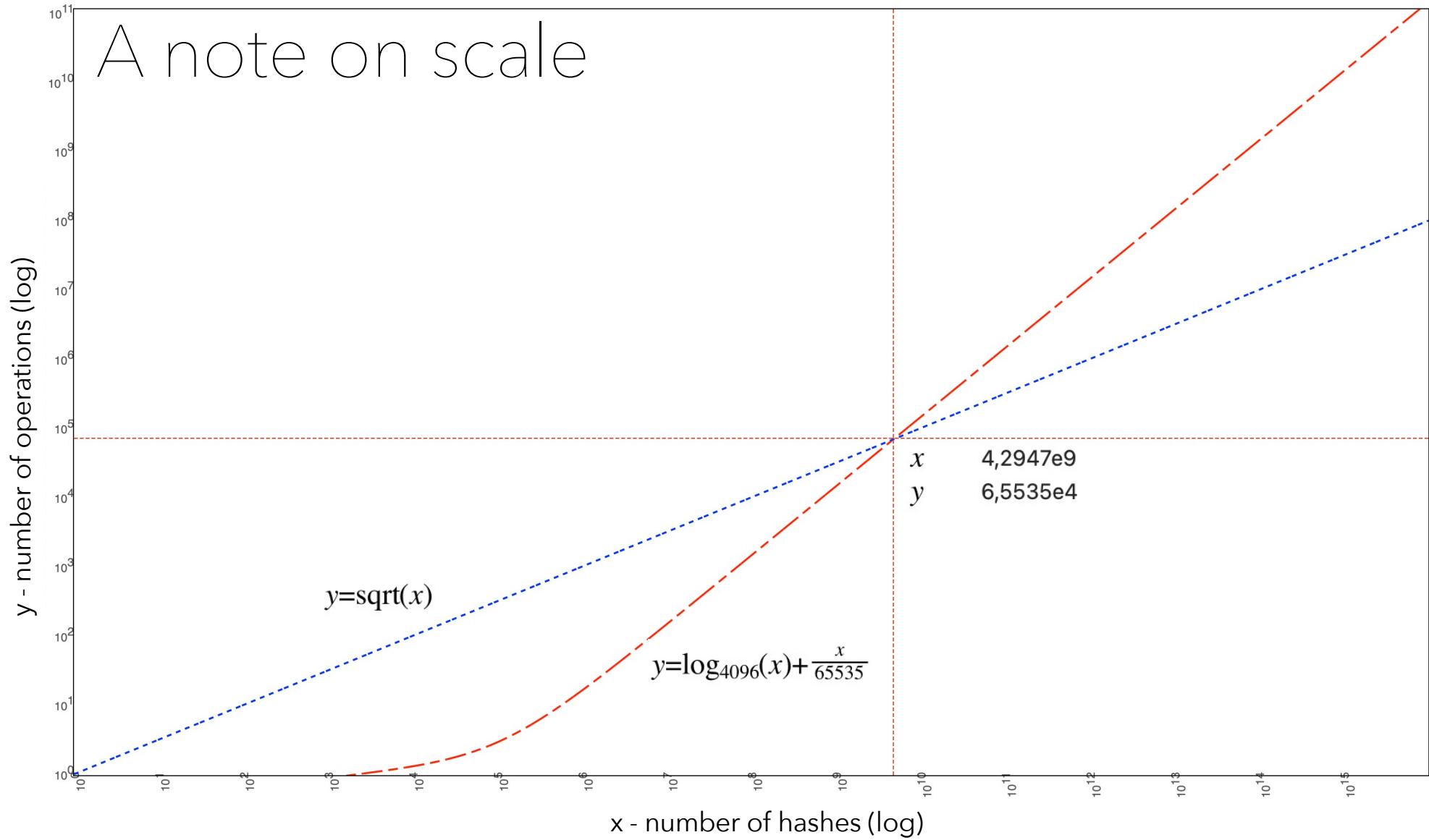
threading

rust!

databases!

two-byte lookups

# A note on scale



# Current (best) Performance

<b>hash</b>	<b>small</b>	<b>rockyou</b>	<b>HIBP</b>
hash1	19ms	19ms	17ms
hash2	11ms	13ms	12ms
hash3	11ms	11ms	63ms

Average: 20ms  
Median: 13ms

# Assless Demo

<https://github.com/sensepost/assless-chaps/>

# Have I Been Pwned HashList Problems

123456 (23.2m)	ashley (432,276)	liverpool (280,723)	blink182 (285,706)	superman (333,139)
123456789 (7.7m)	michael (425,291)	chelsea (216,677)	50cent (191,153)	naruto (242,749)
qwerty (3.8m)	daniel (368,227)	arsenal (179,095)	eminem (167,983)	tigger (237,290_
password (3.6m)	jessica (324,125)	manutd (59,440)	metallica (140,841)	pokemon (226,947)
!!!!!! (3.1m)	charlie (308,939)	everton (46,619)	slipknot (140,833)	batman (203,116)

<https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security>

# Hashcat Generated Hash Lists

Wordlist:

password

company\_name

Rules:

Add Numbers

Add Dates

Change Case

Results:

Password1

Password2

Password2021

AcmeCorp1

AcmeCorp2

AcmeCorp2021

# Hashlist Generation Demo

<https://github.com/sensepost/assless-chaps/>

# Wrap Up – Crackers Paradise

As I iterate candidates in the keyspace of DES  
I take a look at my battery life  
And realise there's not much left  
Cause I've been cracking this hash so long  
That even my momma thinks that my life is gone  
But I ain't never cracked a hash that didn't deserve it  
Hashcat says 25 years, will I ever reach 24?  
The way things are going I don't know

Tell me why are we, so blind to see,  
that a better way to crack,  
is in front of you and me

# Why are we doing this?

To recover an NT hash quickly

But why?

1. To pass the hash to NTLMv1 endpoints
2. To connect to Wi-Fi or PPTP VPNs
3. To host rogue Wi-Fi access points

# In Summary

1. MSCHAPv2 used the NTHash not the clear text password
2. You can use full NT hash lists, including the uncracked
3. New hashcat modes 27000 & 27100 for NTLMv1 & NTLMv2
4. MSCHAPv2 exposes its ass (easy brute of last two bytes)
5. These can reduce the hashlist to crack against
6. Index'ed DB lookups cost less than DES brute-forces
  1. At less than 17 billion hashes (average case)

# Greetz & Shouts

- Orange Cyberdefense Hackathon Team
  - Darryn, Aurelien, Charly
- Atom and Chick3nman for hashcat module writing help
- Joshua Wright for asleap
- Moxie & David for cloudcrack
- Chick3nman for hash shucking
- <https://github.com/sensepost/assless-chaps/>

WANTED

WANTED