Chasing the long tail:

Cracking complex passwords

Phil Trainor

This talk is about hacking people

- Defeating (near) impossible math by better understanding the constant flaw in network security: People
- Why? Because odds are you don’t have: A Cray machine, Access to Bluffdale UT, Endless $$ to buy EC2 resources on AWS

Who am I?

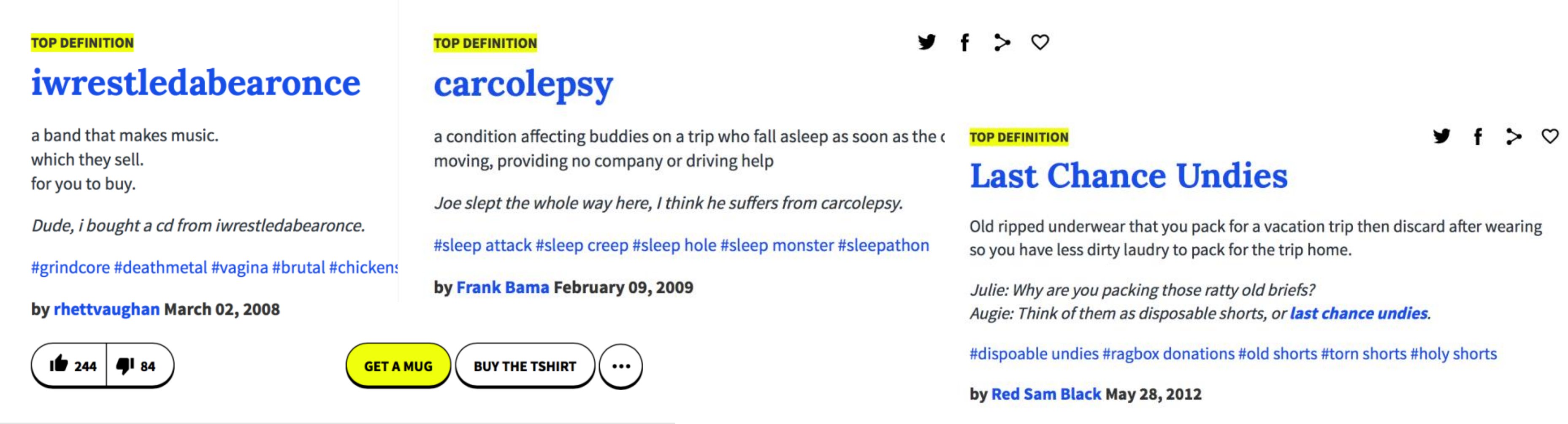
Someone whose cracked a lot of passwords. Many with complexity far beyond my hardware's ability to guess in my lifetime.

In order to crack some of these passwords I had to get creative.

This lecture is about successful techniques….

Urban Dictionary

- Brute forcing with mangled urban dictionary words has yielded an unbelievable number of **impossible** to guess passwords.
- Try the usual suspects first: dictionary words, major lists…
- Complex passwords, that you can remember, are "friend speak" found in Urban Dictionary



TOP DEFINITION

iwrestledabearonce

a band that makes music.
which they sell.
for you to buy.

Dude, i bought a cd from iwrestledabearonce.

#grindcore #deathmetal #vagina #brutal #chicken

by rhettvaughan March 02, 2008

TOP DEFINITION

carcolepsy

a condition affecting buddies on a trip who fall asleep as soon as the
moving, providing no company or driving help

Joe slept the whole way here, I think he suffers from carcolepsy.

#sleep attack #sleep creep #sleep hole #sleep monster #sleepathon

by Frank Bama February 09, 2009

TOP DEFINITION

Last Chance Undies

Old ripped underwear that you pack for a vacation trip then discard after wearing so you have less dirty laudry to pack for the trip home.

Julie: Why are you packing those ratty old briefs?
*Augie: Think of them as disposable shorts, or **last chance undies**.*

#dispoable undies #ragbox donations #old shorts #torn shorts #holy shorts

by Red Sam Black May 28, 2012

How did I come up with this?

- Rockyou, crackstation, darkc0de, single crack, etc were not getting the job done: 30% effective at best
- So….. I thought about my passwords:
  - I had 6 unique passwords (work, email, my servers, …)
  - All passwords derived from “Friend Speak”
  - My wordlists, even with exhaustive rules, would never come close
- The “South Park Movie” was huge when I was in college
- 61ShutYourFuckingFaceUncleFucker!
- 33 characters total:
  - my jersey number in sports ball
  - My base word: Shut Your Fucking Face Uncle Fucker
  - one symbol
- About 3 quindecillion years to crack with GPUs
- My base word is in Urban Dictionary
- John/OclHashCat –wordlist=UD_caps.txt --rules
- My complexity is now 95^4 or 81 million max
- Breakable in 12 minutes (worst case) with my GPU Array

My modus operandi

- Automation: queue every hash/pcap/etc
- Cycle through password lists with no rules
  - US Lists: rockyou, crackstation, darc0de, etc
    - About 100 lists. Around 5 GB of ASCII
    - Hit rate about 25% in US, far less outside
  - Foreign lists: double-byte hex, foreign words, cracked foreign dumps (yandex-ru, etc)
    - About 100 lists. Around 2 GB of ASCII
    - Hit rate about 5%, same outside
- Single Crack Mode with rules
  - Listing email address, username, hometown, etc in john (sadly) yields about 5% hit
  - At this point I've tried about 2 billion guesses with 30% success
- Cycle again through specific lists with rules
  - This is where we separate the women/men from the girls/boys
  - If the quality of "base words" doesn't resemble passwords then you will be wasting electricity with minimal results

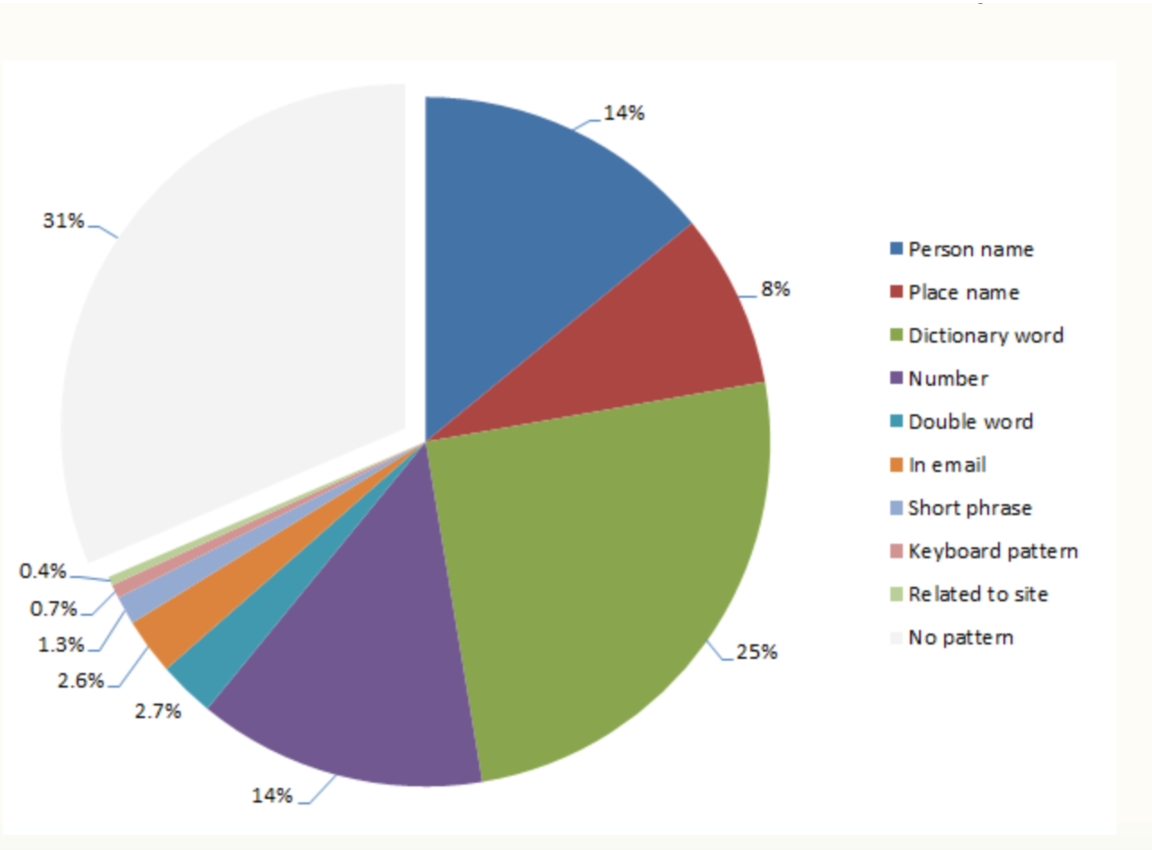
Why do people pick certain passwords?

Troy Hunt wrote a great paper in 2011 on the subject.

I disagree on several points based on my cracking experience.

Maybe the world changed a lot in the last 5 years but:

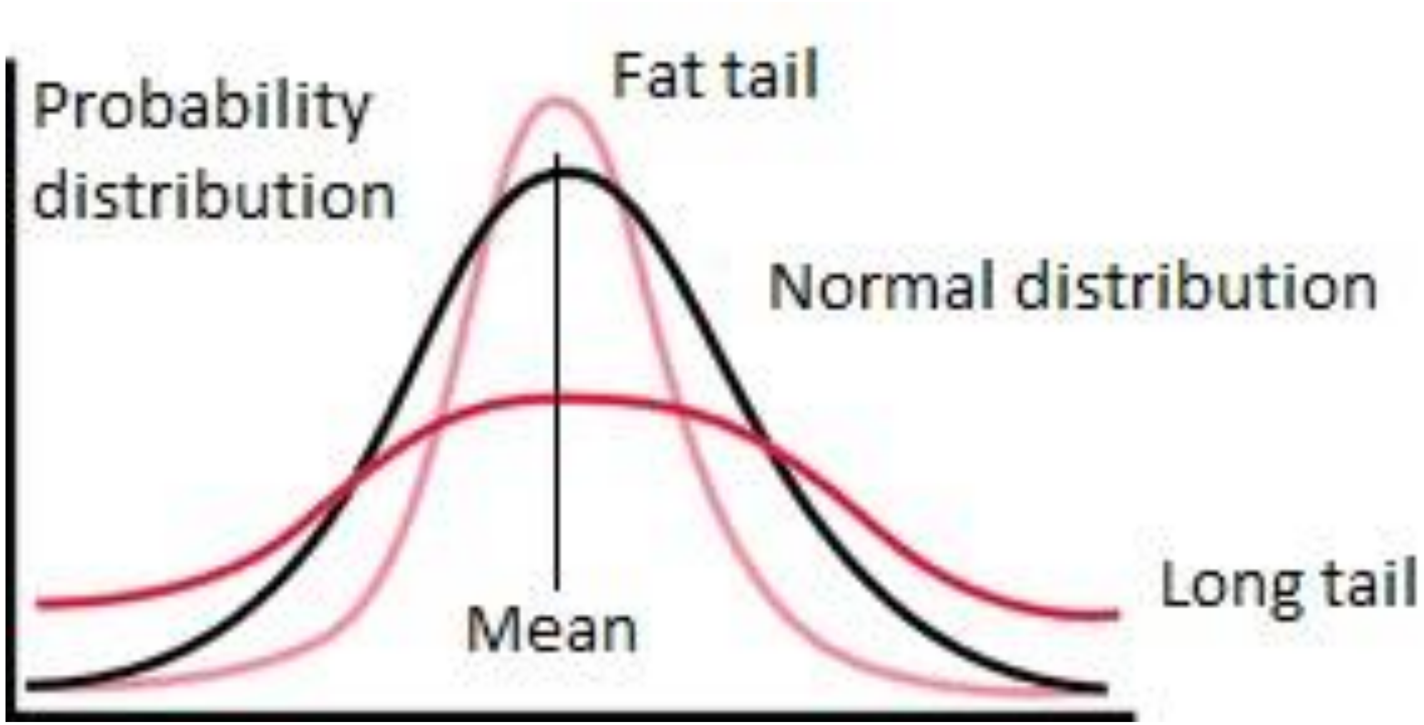
- 25% of passwords are not dictionary words
- **31% of passwords are not patternless nonsense**
- I bet 31% are “friend speak”



https://www.troyhunt.com/science-of-password-selection/

What is “The Long Tail”

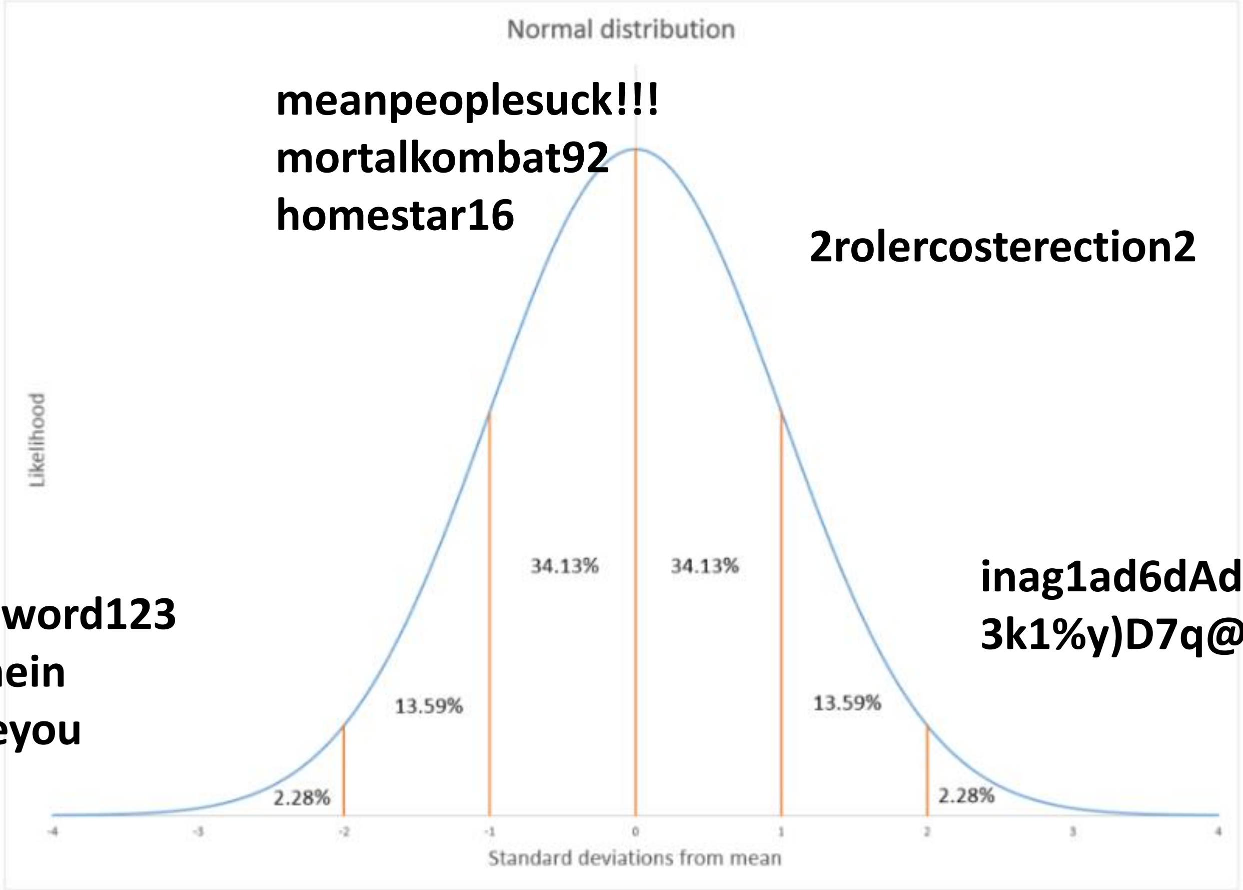
In statistics a long tail of some distributions of numbers is the portion of the distribution having a large number of occurrences far from the "head" or central part of the distribution.



Standard Deviations from Mean

“Tail” passwords are (typically) created as a result of good security practices

- They force minimum complexity standards
- They expire making a brute force operate on a short time table
- Time & Resources are the key component to brute forcing



meanpeoplesuck!!!
mortalkombat92
homestar16

2rolercosterection2

password123
letmein
iloveyou

inag1ad6dAdAv&i$da
3k1%y)D7q@t^

Cracking = Time
Time = Complexity / Resources

Simple Stuff to get out of the way…

- There are 95 printable ASCII characters
- To brute a password that utilises diverse characters = 95^[length of passwd]
- Just lowercase and numbers = 36^[length of passwd]
- With an 8 char passwd the 95 example is 2352 times harder to crack than the 36 example
- With hardware acceleration it’s the difference between a week and several lifetimes
- I recommend GPUs
  - Fast
  - Cheap
  - Most brute force software supports “clustering”

Head Passwords

In password cracking the “**head**” are the easy to crack passwords

- Passwords in major lists
- Passwords with low complexity

Example: Passwords with an affiliation with the user

- Steve went to Umass and graduated in 2009.
- Steve posts lots of old pictures
  - College
  - Sports
  - drinking

Steve picked: zoomass2009
The 5 minutes of research took longer than cracking

Tail Passwords

In password cracking the “tail” are the passwords that employ complexity

- Passwords that are not in lists
- Password mangling rules are ineffective
  - If you don’t have the “base word(s)” mangling just cost electricity with minimal results
- Passwords with high complexity
- Passwords without affiliation with the user

There are 2 types of Tail passwords

1. People who logically can remember multiple passwords in the format: 3k1%y)D7q@t^
   - This is 1% at most
   - The truly paranoid
   - Outside of Bluffdale, UT impossible to guess
2. People who use “friend-speak” i.e. unintelligible non-dictionary idiomatic words that are (sometimes) mangled
   - This is the 31% in Troy Hunt’s model
   - These are words “webster’s dictionary” does not carry
   - Centered around words like “kanyeteruption”: An unwanted and rude disturbance
   - “kanyeteruption” is nonsense but easily remembered and has complexity
   - mangling these types of words will get results

How many standard deviations from the mean?

- Because of guidance from security professionals Steve now picked:
  - z00M@$$2008
- A **<u>much</u>** better passwd
- Still not a “tail” password
- Comprised of “common elements” that can be mangled
  - umass
  - zoomass
  - 2008

Snowden’s (bad) advice

MargaretThatcheris110%SEXY

- Not obscure words: SEXY, IS, Margaret….
- Thatcher is the most obscure but it’s a famous name
  - I have lists that combine and mangle top 4000 common used words (includes margaret, is, sexy)
- Breakable with rules and (good) hardware
- If encrypted with weak math very breakable
  - I count 6 diverse “Elements” i.e 7.35^11 total guesses.
  - I think he counts 26 elements i.e 2.6^51 and impossible to brute
- He should be worried about the NSA, not “some guy with an array of GPUs”

Steve picks a “tail” password

- “Steve” picked “3k1%y)D7q@t^“ for his passwd.
- 12 unique elements
- No amount of mangling will improve odds
- 5.4036E+23 complexity

Combinations	**5.4036E+23**	**seconds in hr**	**3600**
guesses per second	**1000000000**	**seconds in day**	**86400**
		seconds in year	**31557600**
		seconds in	**3155760000**
time to crack in seconds	**1.501E+11**	**millenia**	**0**
time to crack in days	**6254167681**		
time to crack in years	**17122977.91**		
time to crack in milenia	**17122.97791**		

If during the Miocene epoch, the first ancestors of humans who evolved from chimpanzees started cracking at 1 billion guesses per second they would have tried the last combination today.

Steve can’t remember “3k1%y)D7q@t^“

How do normal people pick “Tail” passwords

- We are not normal
- In college one of my CompSci prof’s told us “we are not normal”
- The way we think fundamentally differs from a huge percentage of the population

Now that I’m 15 years out of university this may no longer be true

- If you are under 25 you grew up with the internet
- If you are under 25 you grew up managing online accounts
- If you are under 25 you have a different perspective

Millions of these words..

- **trumperbate**: The act of delusionally self-rewarding oneself for the occurrance of a terrible event by publicly masturbating while simultaneously spamming Twitter.
- **Netflix and Chill:** Go over to your partners house and fuck with Netflix in the background.
- **opooportunity:** When one who has to defecate has an opportunity to relieve themselves after waiting for a period of time.
- **Handcestors:** all the ancestors never to be born due to male masturbation.
- **On My Michelle Obama:** Used in Fifth Harmony's song “BO$$”, has a similar meaning as fleek but also involves having a healthy body and diet of vegetation.
- **Margaret Thatcher:** Evil Emperess of Britain between 1979 - 1990. Eventually thrown down a mine shaft by Darth Heseltine in a leadership contest.

“Margaret Thatcher” AND “On My Michelle Obama”: Urban Dictionary would seriously mess with Snowden’s password suggestions…

There are also a few dozen words similar to “Margaret Thatcher”... some are rather disgusting.

Don’t forget Urban Dictionary User Names…

- mamasquat
- Idonlikepudding
- Margaret Thatcher's Dog
- Beckburris23
- Ronin Catholic
- Octopimpslap
- JumpingMafu
- Argonator
- pazlittlesong
- Gaberhamthinkin

- These names are also in the category of “Friend-Speak”
- Complex idiomatic words that are not in dictionaries and (largely) not in password lists

Margaret Thatcher's Dog…

The Password doesn’t comply?!?!?!

- User can remember “netflix and chill”
- It has more than 8 characters
- But it was rejected due to lowercase & lacking non-alphas
- **What will the user do?**
- As little as possible to comply:
  - Throw in a number
    - Let’s put it at the end; easier to remember
  - Capitalize something
    - It’s going to be the ‘N’ or the ‘C’
  - A freaking symbol?!?!
    - That goes on the end too so it won’t mess with my core concept

User’s new password is: **NetflixandChill34!**

How complex does Snowden's passwd look now?

MargaretThatcheris110%SEXY

Sports Illustrated
Prime location
Maggie Thatcher Melts Mauritius
Laetitia Casta, Castaway in Cameron
FreakingNews.com

You're now cracking with Urban Dictionary

The password isn't close to bulletproof

Ciphers Matter

- Certain Ciphers (obviously) add an inexorable amount of time to the crack
- bycrypt is a great example: Loop Iterations inhibit brute attempts
- WPA2 PSK is easy with GPU: no loop iterations ☺
- Mr. Robot was intimidated by WPA and went for another route to breach the Dept of Corrections
- Let’s discuss…

I know, it’s TV… but still…

- Let’s assume the police on Mr. Robot was using WPA2 with PSK and not Active Directory
  - Elliot would have said they authenticate with AD and not imply brute force was an option
- A good, single GPU can guess 100K WPA2 combinations per second
  - OclHashCat and Pyrit do a great job of clustering GPUs
  - 10 Billion Guesses in 6 hours is not unreasonalbe
- 99% of police work is talking to people
  - They need a PSK they can remember
  - It will be derrived from “Cop Lingo”
  - Where do we have a great list of colloquial metaphors???
  - **Urban Dictionary**

So… how to pick passwords

- “Friend-speak” as your base is not safe
- Idioms are not safe
- Personally, I cannot remember multiple variants of 3k1%y)D7q@t^

What would be a really strong password?

- In 1968, Iron Butterfly’s singer, Doug Ingle, was so drunk he slurred his own lyrics and created “In-A-Gadda-Da-Vida”
- No one had ever strung those 18 ASCII characters together before, EVER.
- **Unintelligible nonsense that ONLY YOU have ever come up with in the history of mankind that <u>you can remember</u>.**
- Sprinkle Caps, numbers, symbols
- If no one made an alcohol run to that studio in 1968 you could have used:
- **inag1ad6dAdAv&i$da**

But they did, so you can’t use it. It’s also on a slide in DefCon Archives…

Iron Butterfly

Thank You!!