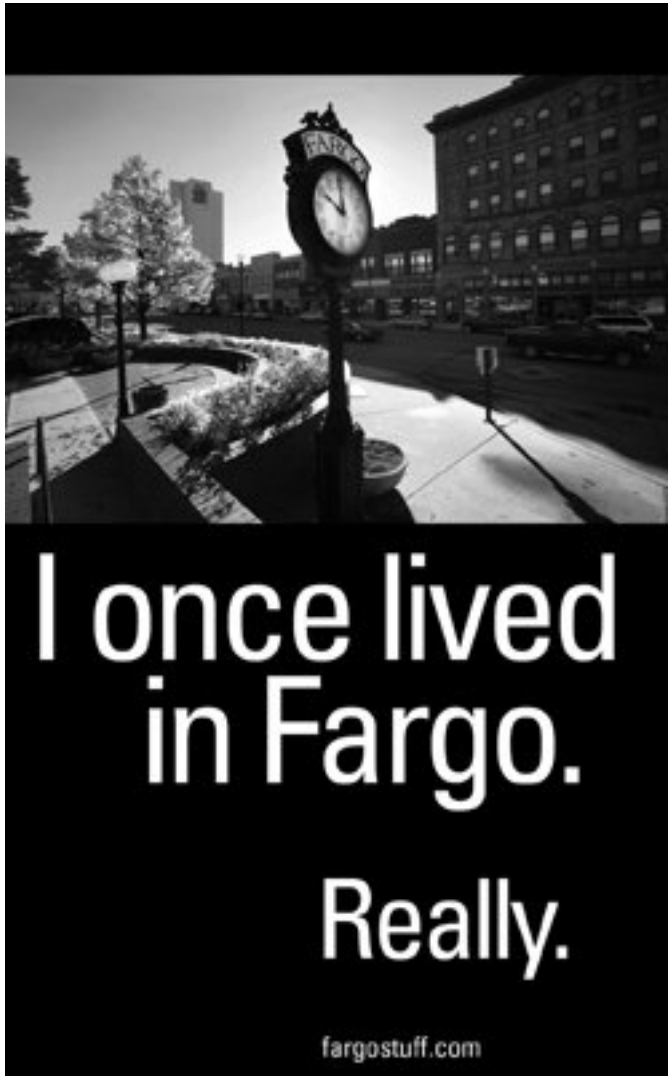
Password Cracking

About me

- Originally from Fargo, ND
- Came down to DSU in 2007
  - B.S. Computer & Network Security
  - Minor in Networking
  - M.S. Information Assurance
  - D.Sc. Cyber Operations (working on it)



Security Work

- Web Application/Software Developer (2008)
- Network Administrator (2010)
- Security Consultant (2011)
  - Worked for a large firm in Fargo, ND for about three years
- Independent Security Consultant (current)
- Instructor at DSU (current)

- You'll l … v you how to …
- You wi … at you don't c …
  - Not a …

Legitimate Password Cracking

What makes a strong password?

- Length (total number of characters)
- Complexity
  - Upper/lower case
  - Numbers
  - Special characters
- Frequency of change
  - If it takes you 60 days to crack my password, and I change it every 59…guess what?

How do attackers break passwords?

- Really not a trick question, just want to know what you guys think.

Two Main Categories

- Online
  - Trying to authenticate to a real service with a live, active account
  - Sitting down in front of your buddy's computer and trying to log in to their FaceBook account
- Offline
  - Getting a secure password value, taking it back to your own computer, and trying to breakit

How about a brute-force attack?

- Systematically guessing every possible combination until you get the correct answer


Yale

Calculating Character Space

- In passwords, we can reuse characters
- Determine the number of allowed characters
  - Just lowercase: 26 total
  - Upper/lower: 52 total
  - Add in numbers (0-9) 62 total
- Figure out how long the password is
- Raise the number of allowed characters to the power of the length of the password
- (Character Space)^Length

Calculating Character Space

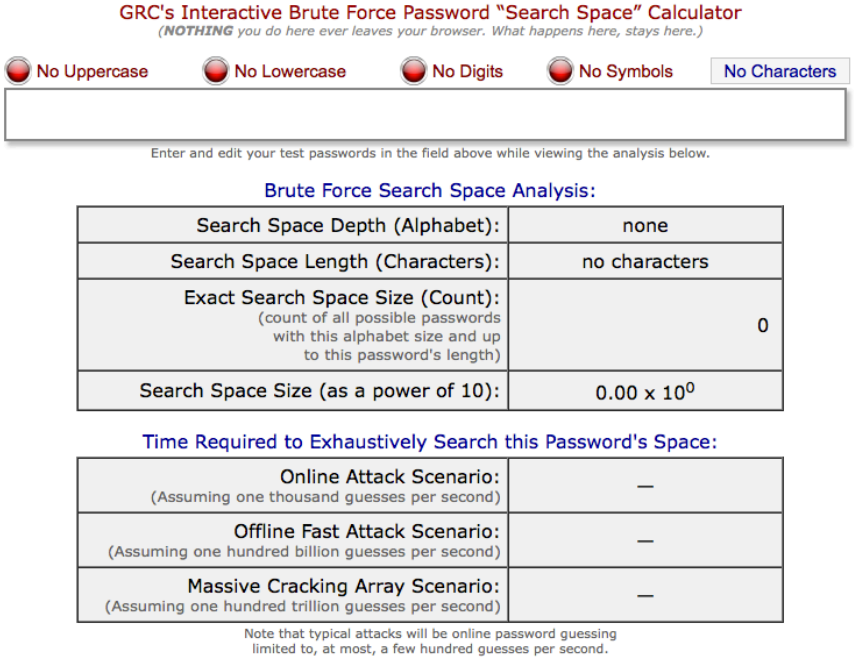
- What if you can only use numbers for your password
  - Numbers 0-9, count them, there's **10** possibilities
- If your password is **1234** (length of 4)
- We can take 10*10*10*10 or **10^4**
- There's only about **10,000** possibilities

Calculating Character Space

- A bit more complex…
- 26 upper case + 26 lower case = **52** total
- My password is **Password** (8 characters long)
- 52*52*52*52*52*52*52*52 or **52^8**
- 52^8 = **53,459,728,531,456**
  - Fifty-three trillion possible combinations

https://www.grc.com/haystack.htm

- Password Haystack – how long will it take to brute force your password?



GRC's Interactive Brute Force Password "Search Space" Calculator

*(**NOTHING** you do here ever leaves your browser. What happens here, stays here.)*

No Uppercase | No Lowercase | No Digits | No Symbols | No Characters

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	none
Search Space Length (Characters):	no characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	0
Search Space Size (as a power of 10):	0.00×10^0

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	–
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	–
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	–

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

GRC's Interactive Brute Force Password "Search Space" Calculator

*(**NOTHING** you do here ever leaves your browser. What happens here, stays here.)*

No Uppercase | 5 Lowercase | No Digits | No Symbols | 5 Characters

cyber

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26
Search Space Length (Characters):	5 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	12,356,630
Search Space Size (as a power of 10):	1.24×10^7

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	3.43 hours
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	0.000124 seconds
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	0.000000124 seconds

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

GRC's Interactive Brute Force Password "Search Space" Calculator

*(**NOTHING** you do here ever leaves your browser. What happens here, stays here.)*

1 Uppercase | 4 Lowercase | No Digits | No Symbols | 5 Characters

Cyber

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+26 = **52**
Search Space Length (Characters):	5 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	387,659,012
Search Space Size (as a power of 10):	3.88×10^8

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	4.49 days
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	0.00388 seconds
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	0.00000388 seconds

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

GRC's Interactive Brute Force Password "Search Space" Calculator

*(**NOTHING** you do here ever leaves your browser. What happens here, stays here.)*

1 Uppercase | 3 Lowercase | 1 Digit | No Symbols | 5 Characters

Cyb3r

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+26+10 = **62**
Search Space Length (Characters):	5 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	931,151,402
Search Space Size (as a power of 10):	9.31×10^8

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	1.54 weeks
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	0.00931 seconds
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	0.00000931 seconds

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

GRC's Interactive Brute Force Password "Search Space" Calculator

*(**NOTHING** you do here ever leaves your browser. What happens here, stays here.)*

1 Uppercase | 2 Lowercase | 1 Digit | 1 Symbol | 5 Characters

(Yb3r

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+26+10+33 = **95**
Search Space Length (Characters):	5 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	7,820,126,495
Search Space Size (as a power of 10):	7.82×10^9

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	2.98 months
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	0.0782 seconds
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	0.0000782 seconds

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

GRC's Interactive Brute Force Password "Search Space" Calculator

*(**NOTHING** you do here ever leaves your browser. What happens here, stays here.)*

1 Uppercase | 14 Lowercase | 4 Digits | 5 Symbols | 24 Characters

I love cyber stars 2014!

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+26+10+33 = **95**
Search Space Length (Characters):	24 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	295,095,290,555, 142,625,648,321,021,999, 764,315,625,454,517,120
Search Space Size (as a power of 10):	2.95×10^{47}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	93.83 billion trillion trillion centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	9.38 hundred trillion trillion centuries
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	9.38 hundred billion trillion centuries

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

Brute-force

- Ok, sweet. We can take every possible combination, but what are some problems with it?
  - Takes forever
  - Account lockouts – does your bank allow you to fail logging in 100 times
  - For most things, it's really not that practical

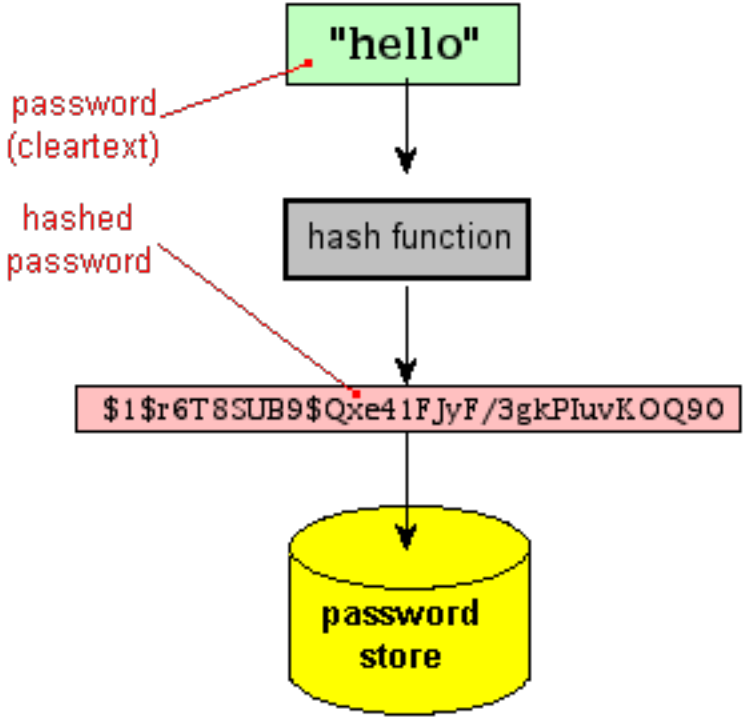
How are passwords stored?

- Windows and *most* websites don't actually store your password as a humanly readable word
  - If the system or their database get's pwned, they're in a world of hurt
- Hashes
- Salted Passwords

Password Hash

- A hash is a one-way, non-reversible way to store some sort of data
  - Anyone used MD5, SHA1
- To authenticate a user, the password presented by the user is hashed and compared with the stored hash
  - Can't get the password back from a hash

Hashing


"hello"
password
(cleartext)
hashed
password
hash function
1r6T8SUB9$Qxe41FJyF/3gkPIuvKOQ90
password
store

Windows Password Hashes

- Windows stores user passwords in the system's password database (called "SAM") in an encrypted hash
- LM Hash – old and really broken
  - Windows XP = Easy!
  - Windows Vista and above – turned off by default
- NTLM Hash – new and not as broken
  - Used in Windows Vista and above

LM Hash Major Flaws

- Password is restricted to a maximum of fourteen characters
- Password is converted to uppercase
- This password is null-padded to 14 bytes
- The “fixed-length” password is split into two seven-byte halves

NTLM Hash

- NTLM is case sensitive
- Character set is 65,535, and it does not limit stored passwords to two 7-character parts
- Considered a much stronger hashing algorithm
- Same concept in the end, just harder to break

Hashes

- LM
  - 855c3697d9979e78ac404c4ba2c66533
- NTLM
  - NT7f8fe03093cc84b267b109625f6bbf4b
- Bunch of sample hashes:
  - http://openwall.info/wiki/john/sample-hashes

Getting a Password Hash

- PW Dump
- Cain & Able
- FG Dump
- Get a root shell on the machine remotely, and use some 1337 tools in Kali to extract them

Ok, we have the hashes…

- Now, it's time to break them
- We can start by brute-forcing some

```
Administrator:500:NO PASSWORD**********************:31D6CFE0D16AE931B73C59D7E0C089C0:::
Guest:501:NO PASSWORD**********************:NO PASSWORD**********************:::
DSU:1000:NO PASSWORD**********************:7FACDC498ED1680C4FD1448319A8C04F:::
Ricky:1098:8C6F5D02DEB21501AAD3B435B51404EE:E0FBA38268D0EC66EF1CB452D5885E53:::
Bubbles:1099:E52CAC67419A9A224A3B108F3FA6CB6D:8846F7EAEE8FB117AD06BDD830B7586C:::
Julian:1100:0222C809FA6E75161CE9CD479353E782:0FB7F09F6B46A6E019B5999572F1AC4E:::
Barb:1101:05083E9CECF981D65E57FC0295493699:2718034A5D4AAE8FD80A621322A0AB51:::
Dennis:1102:NO PASSWORD**********************:0AE8809CAB6D0CF7FC049790D14AA16D:::
```

John the Ripper

john --user:**<username> <hash file>**

NOTE: The user name is case sensitive!

Even Easier

Dictionary Attacks

- Attackers are pretty smart
- Once you break a bunch of passwords, why not write them down
- Compile a huge list of passwords that people actually use
- Try each of those hashes to see if they're the right one

RockYou.txt

- In 2009, a major password breach occurred
- 32.6 million stolen passwords of the website's users disclosed
- Attackers have grabbed this, and added to it
- http://cyberstars.ialab.us/Password_Kitteh/

John the Ripper

john --user:**<username>** --wordlist:**<dictionary file>** --**<hash file>**

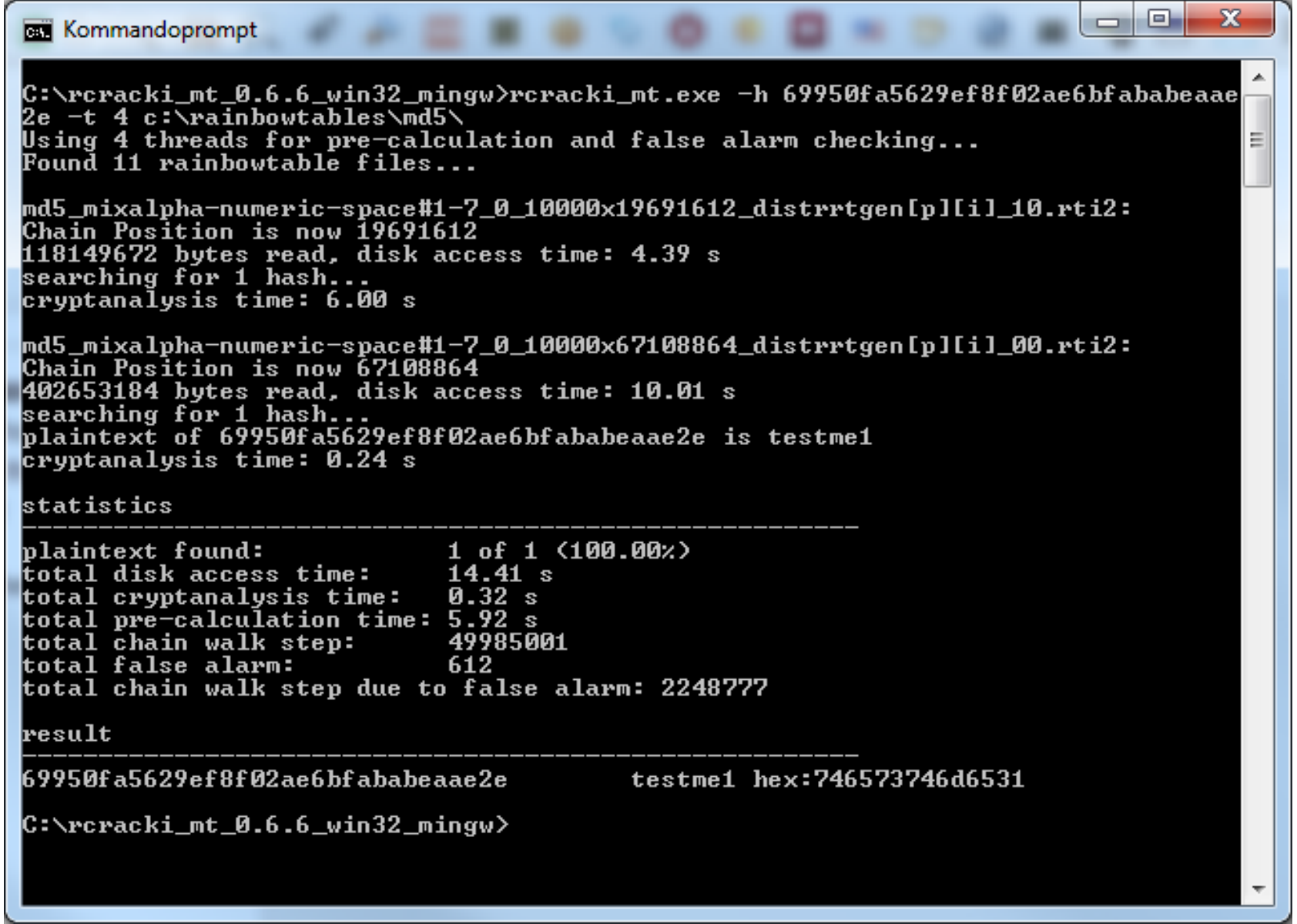
NOTE: The user name is case sensitive!

Rainbow Tables

- Precomputed table for reversing cryptographic hash functions, usually for cracking password hashes
- Using less computer processing time and more storage than a brute-force attack
- More processing time and less storage than a simple lookup table with one entry per hash

Rainbow Tables

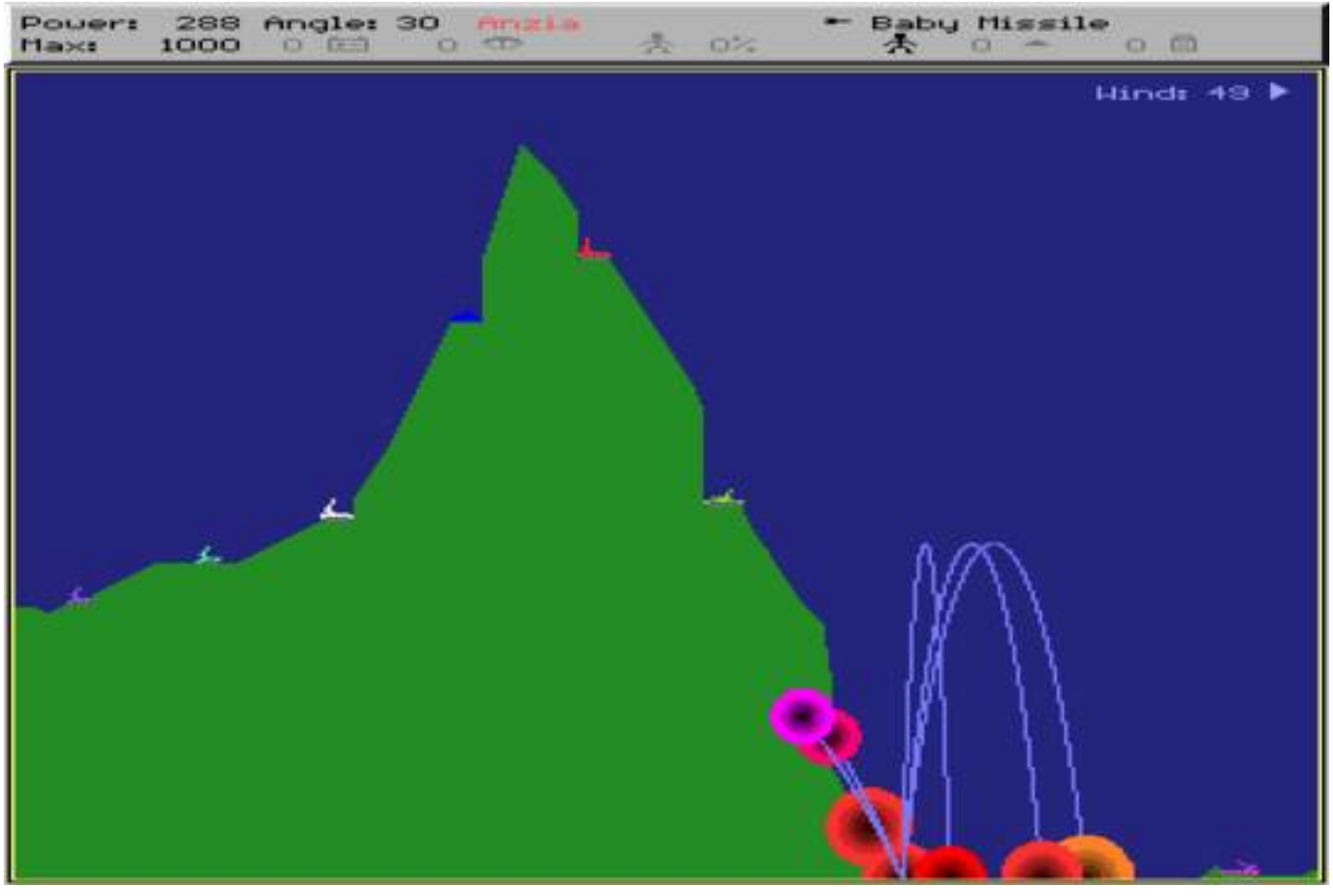
- To store every single 7 character password possible for the given example, it would require a least 417 TB of space - rainbow tables only need around 80 GB of storage space, depending on your generation options
- Middle ground between brute force and dictionary attack
- https://www.freerainbowtables.com


Kommandoprompt
C:\rcracki_mt_0.6.6_win32_mingw>rcracki_mt.exe -h 69950fa5629ef8f02ae6bfababeaae
2e -t 4 c:\rainbowtables\md5\
Using 4 threads for pre-calculation and false alarm checking...
Found 11 rainbowtable files...
md5_mixalpha-numeric-space#1-7_0_10000x19691612_distrrtgen[p][i]_10.rti2:
Chain Position is now 19691612
118149672 bytes read, disk access time: 4.39 s
searching for 1 hash...
cryptanalysis time: 6.00 s
md5_mixalpha-numeric-space#1-7_0_10000x67108864_distrrtgen[p][i]_00.rti2:
Chain Position is now 67108864
402653184 bytes read, disk access time: 10.01 s
searching for 1 hash...
plaintext of 69950fa5629ef8f02ae6bfababeaae2e is testme1
cryptanalysis time: 0.24 s
statistics
plaintext found: 1 of 1 (100.00%)
total disk access time: 14.41 s
total cryptanalysis time: 0.32 s
total pre-calculation time: 5.92 s
total chain walk step: 49985001
total false alarm: 612
total chain walk step due to false alarm: 2248777
result
69950fa5629ef8f02ae6bfababeaae2e testme1 hex:746573746d6531
C:\rcracki_mt_0.6.6_win32_mingw>


CloudCracker :: Online Hash Cracker
https www.cloudcracker.com
Reader
CloudCracker
An online password cracking service for penetration testers and network auditors who need to check the security of WPA protected wireless networks, crack password hashes, or break document encryption.
Start Cracking
File Type
WPA/WPA2
Handshake File
Choose File
no file selected
SSID (Network Name)
Next »
Handshake
Dictionary
Delivery
Save Money. Save Time.
Comprehensive Dictionaries.
Big. Fast. Cheap.
Run your network handshake against
300,000,000 words
in 20 minutes
for $17.
"Welcome to the future: cloud-based WPA cracking is here!" -
- TechRepublic
"Low cost service cracks wireless passwords from the cloud..." -
- TheRegister
"This really is a great idea." -
- Hacker News

GPU vs. CPU

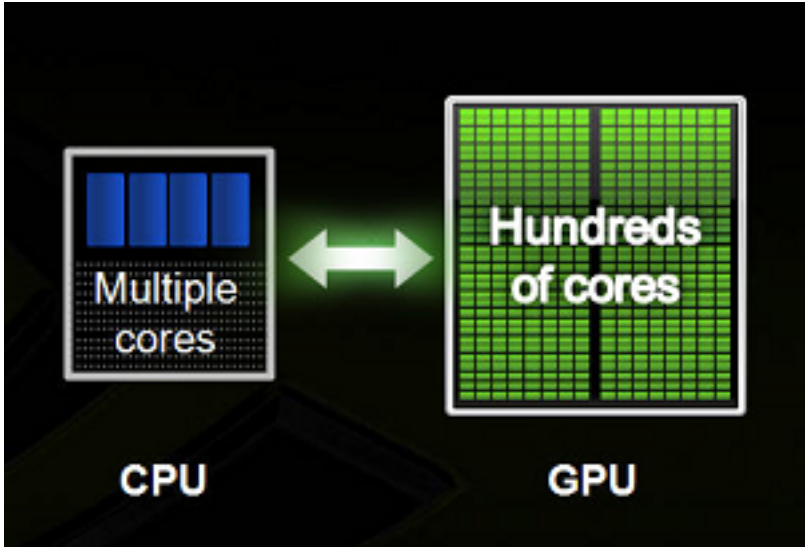
- Any gamers in here?
- I bet if you're 1337, you have a nice graphics card
  - You want full FPS, 1080 resolution, etc.
- What a GPU really does is alleviate some of the load of the CPU and handles some computation for the output on the screen


Power: 288 Angle: 30 Anzia
Max: 1000
Baby Missile
Wind: 49

GPU vs. CPU

- CPU has only few cores/ multiple cores with lots of cache memory that can handle few software threads at a time

- GPU has hundreds of cores that can handle thousand of threads simultaneously



GPU vs. CPU

- GPUs are highly specialized in number crunching, something that graphics processing desperately needs
- Multiple GPUs can also be employed to achieve a single goal
- TL;DR; GPUs are really fast, but designed for very specific types of applications

Not all GPUs are created equally…

- Some graphics cards are more capable than others
- Look at how many cores they have
- How much memory
- Before you go buy a password cracking machine, do your due diligence!


msi
Twin Frozr

Hurdles

- What about non-English passwords?
- Those that use special character sets
  - Wingdings anybody?
  - ⌖♓■♑♎♓■♑’♦ ♋■♲♌□♎♲✍
- Change frequency
- Locking accounts out

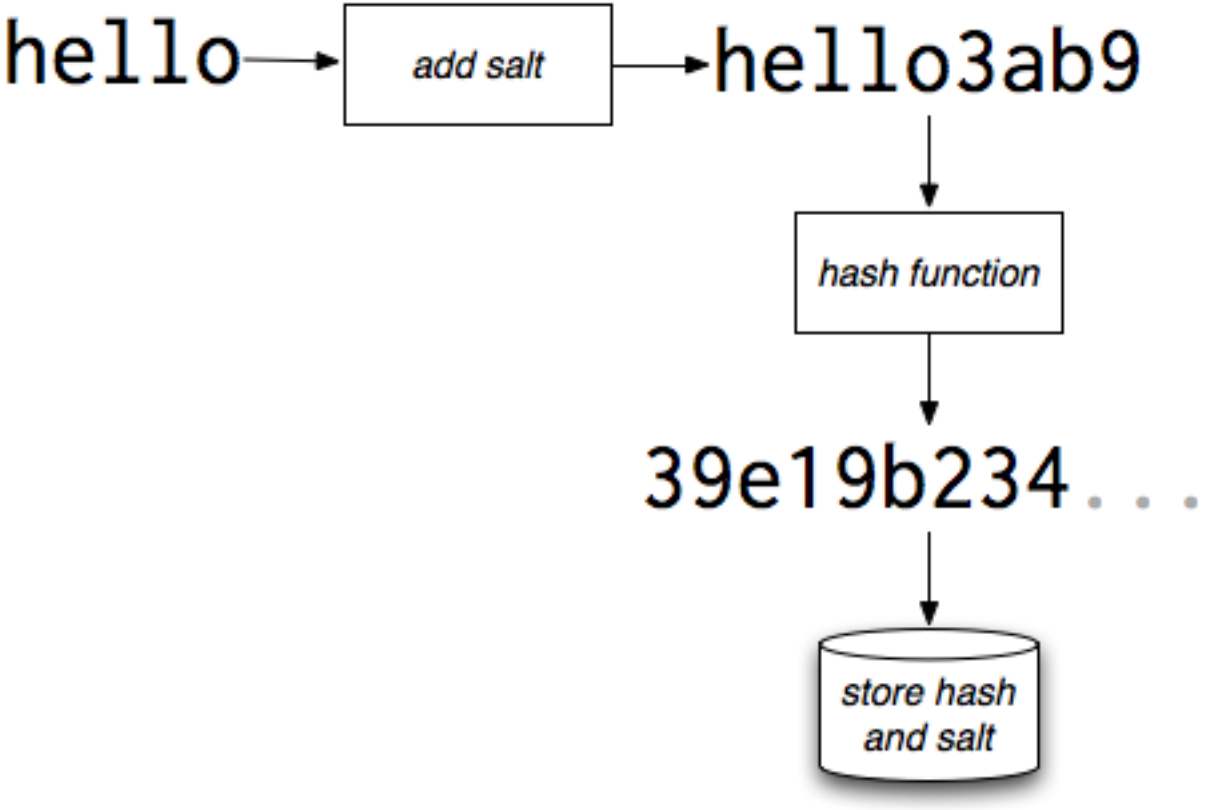
More Iterations

- Running a hash through the hashing algorithms multiple times
- Running a password through SHA256, for instance, and then feeding the hashed output back through the algorithm another 500 times would certainly make wordlist and brute force attacks slower

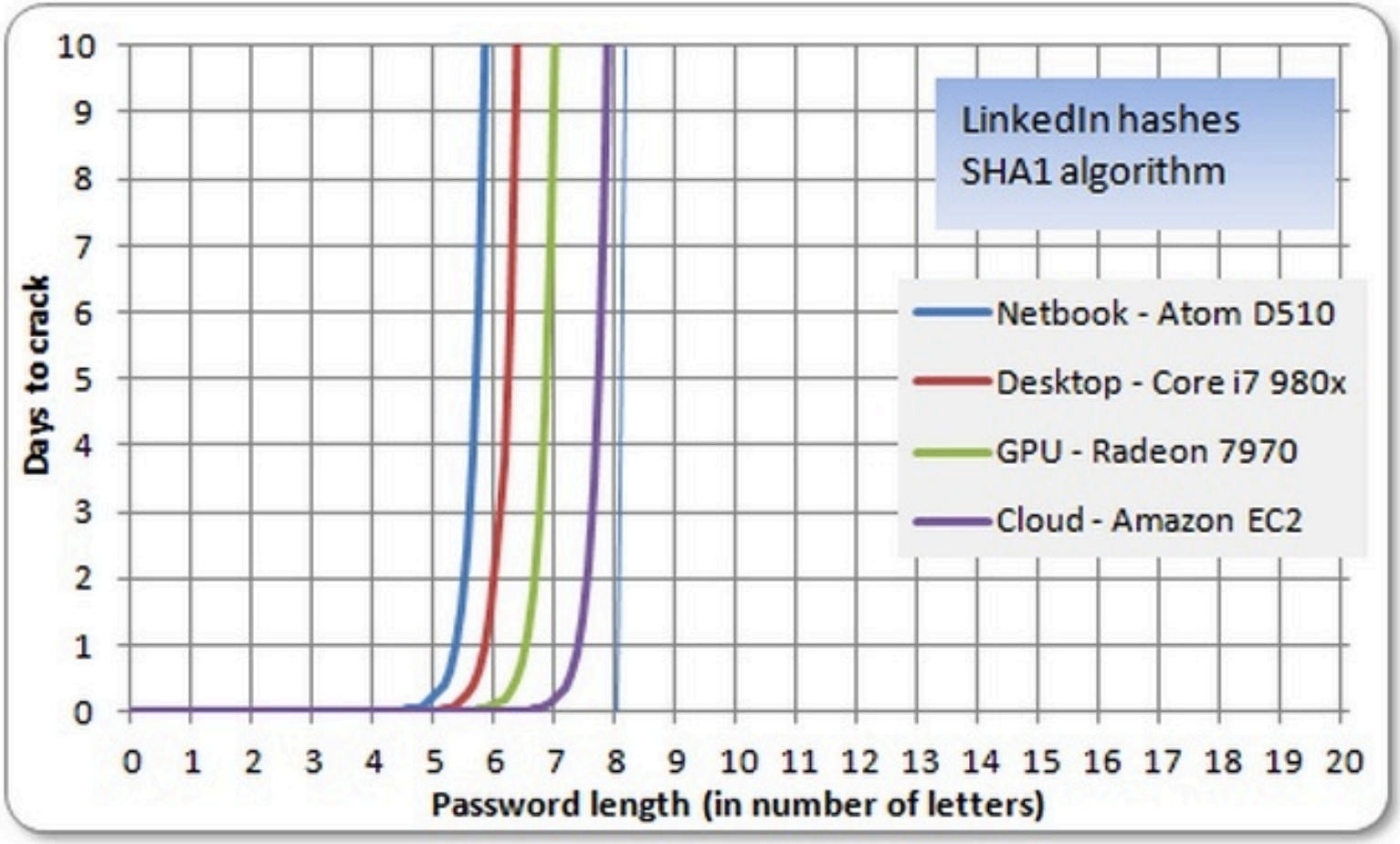
Salting

- Salting attempts to defeat table lookup attacks by adding several characters to the password before passing it through the hashing algorithm
- Characters don't have to remain secret
- Salting also thwarts cracking techniques that rely on rainbow tables

Salting


hello
add salt
hello3ab9
hash function
39e19b234...
store hash and salt

Length


LinkedIn hashes
SHA1 algorithm
Netbook - Atom D510
Desktop - Core i7 980x
GPU - Radeon 7970
Cloud - Amazon EC2
Days to crack
Password length (in number of letters)
0 1 2 3 4 5 6 7 8 9 10
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Multifactor Authentication

- Something you **know**
- Something you **have**
- Something you **are**

Multifactor Authentication

Google Authenticator