

Anatomy of a Password

Robert Andrews, Managing Consultant

Terry Ford, Senior Managing Consultant

IBM i Security, robert.andrews@us.ibm.com, taford@us.ibm.com

October 19, 2016



Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. **No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access.** IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. **IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.**



IBM Security

Agenda

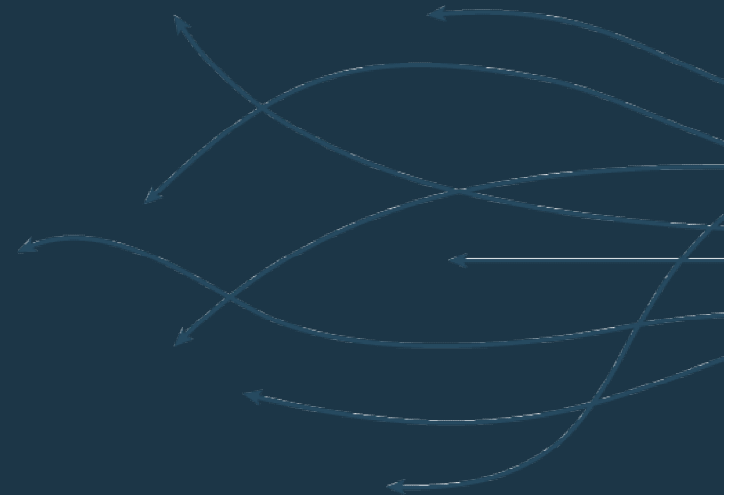
- Password History
- Password Levels on IBM i
- Password Rules
- Password Attacks
 - Dictionary Attacks
 - Brute Force Attacks
 - Other Attacks
- Putting it All Together



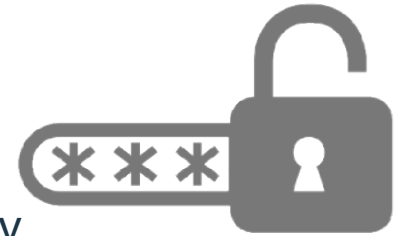


LOOKING BACK TO LOOK AHEAD

Password History



Password History



- Used since ancient times to prove identity, membership, or loyalty
- In computers, dates to 1961 and MIT's CTSS – Compatible Time-Sharing System
 - First password hack was in 1962 by a CTSS user that wanted more time than allocated
- Can be stored in plain text (actual value) or hashed (one way encoding function)
 - Most systems store a hashed version of the password
 - At log in, the user provided password is also hashed and the hashed values are compared to see if they are a match
 - In a secure system, the hash cannot be undone or reversed to the password
 - If a system can ever “recover a lost password” and show you your existing password, it is NOT secure
- What was once considered secure, has been weakened with modern technology
- Newer, better methods exist but are not being widely adopted
- We must change to stay safe!

Password Security Considerations

- Some factors that go into password security include:
 - Storage methods
 - Length
 - Minimums
 - Maximums
 - Character set
 - Digits
 - Alphabetic
 - Special characters
 - Multiple factors
 - What you know
 - What you have
 - What you are
 - Number of uses allowed
 - Single use passwords
 - Password verification mechanisms
 - Is the password ever transmitted?





EXPAND YOUR HORIZONS

Password Levels on IBM i



Password Levels on IBM i

- The IBM i has 4 levels of passwords
 - Current levels are 0, 1, 2 and 3
- Levels 0 and 1 are grouped and levels 2 and 3 are grouped based on character set
 - Levels 0/1 use 26 UPPER case letters, 10 digits, and 4 special characters (\$@#_) only
 - Levels 2/3 use 26 UPPER and 26 lower case letters, 10 digits, 32 special characters and space, recommended
- Levels 0 and 2 are grouped and levels 1 and 3 are grouped based on NTLMv1 passwords storage (used to connect from Windows 95/98/ME clients only without modification)
 - Levels 0/2 do store NTLMv1 passwords, considered hackable and a risk
 - Levels 1/3 do not store and remove NTLMv1 passwords, recommended

Password Level	40 Character Set	95 Character Set
Stores NTLM	0	2*
Discards NTLM	1*	3**

*Recommendations



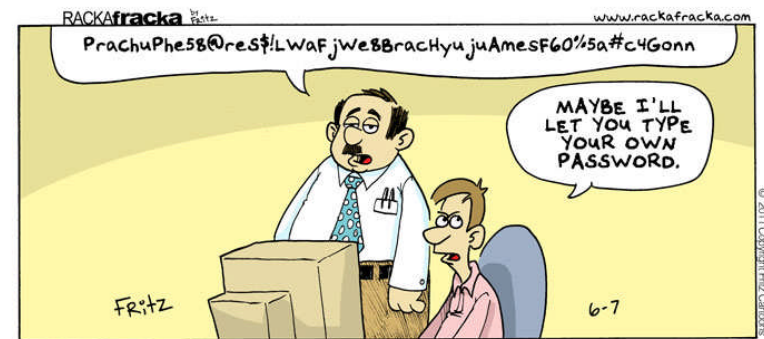
ONE RULE TO RULE THEM ALL?

Password Rules



Password Rules

- In an attempt to make passwords attack resistant, most systems allow administrators to set a list of rules that passwords must follow
- On IBM i we offer several rules:
 - Password Expiration Intervals
 - Minimum length
 - Maximum length
 - Minimum number of alphabetic characters
 - Minimum number of digits
 - Minimum number of special characters
 - Limited repeated prior password
 - Limit position of digits or special character
 - Limited repeated character or consecutive digits
- But do these rules really help prevent or help simplify attacks?





YOUR PASSWORD DOESN'T STAND A CHANCE

Password Attacks



Password Attacks

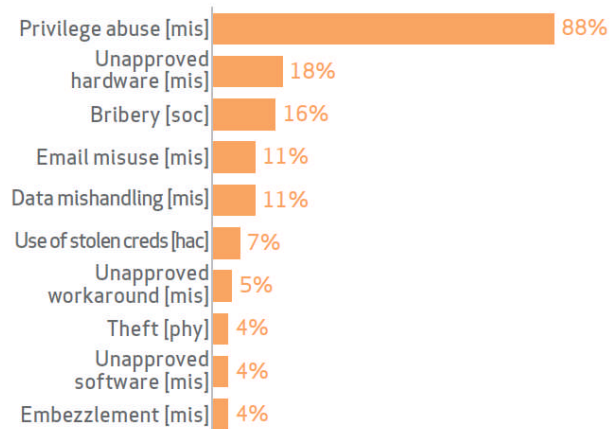


- Passwords are constantly under attack
- Each time a new attack method is developed, systems must change to protect against them
- Most systems today store password hashes as opposed to the password itself
 - This is true on IBM i – we store passwords as a one-way hash
- Most systems today provide a way to access and export those hashed passwords
 - This is true on IBM i – we provide an API to retrieve the hashed password
- This way, the attack can take place on a remote system as to not trigger disabling mechanisms for invalid guesses or attempts
 - This is true of IBM i – can use the exported data to test on another system!
- Since one-way hashes prevent reversing the hash into the password, most attacks are guessing attacks – take a guess at a password, hash it, and compare the two hashes (guess hash vs. retrieved hash) – if they match, you guessed the correct password
 - Possible but unlikely to have a “hash collision” – two different input values that hash to the same result

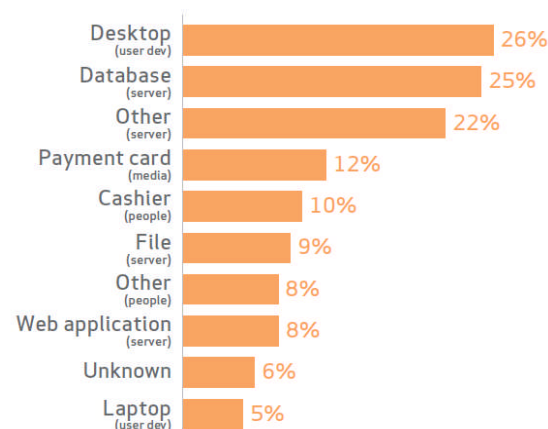
Password Attacks, cont.

- To retrieve the stored, hashed password on IBM i (via the Retrieve Encrypted User Password QSYRUPWD API) you must have *ALLOBJ and *SECADM special authority
- SAVSYS and SAVSECDDTA also conveniently move all hashed passwords to tape!
- If the attacker has *ALLOBJ and *SECADM authority already, why hack the password?
 - Users, even admins, tend to reuse the same password on multiple systems
 - The other user may have accounts on other IBM i systems to which the attacker does not have access or does not have high enough authority
 - And on multiple types of service!
 - Could you access their Gmail? Encrypted documents or file shares?

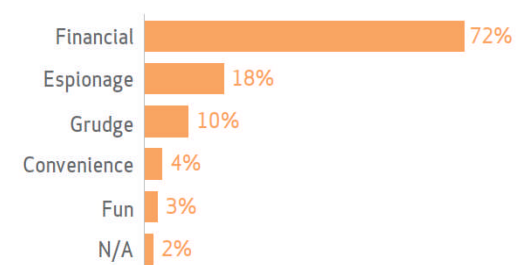
Top 10 threat action varieties within Insider Misuse (n=153)



Top 10 assets affected within Insider Misuse (n=142)



Actor motives within Insider Misuse (n=125)



Source:
2014 Verizon Data
Breach Investigations
Report



LOOK THEM UP!

Dictionary Attacks



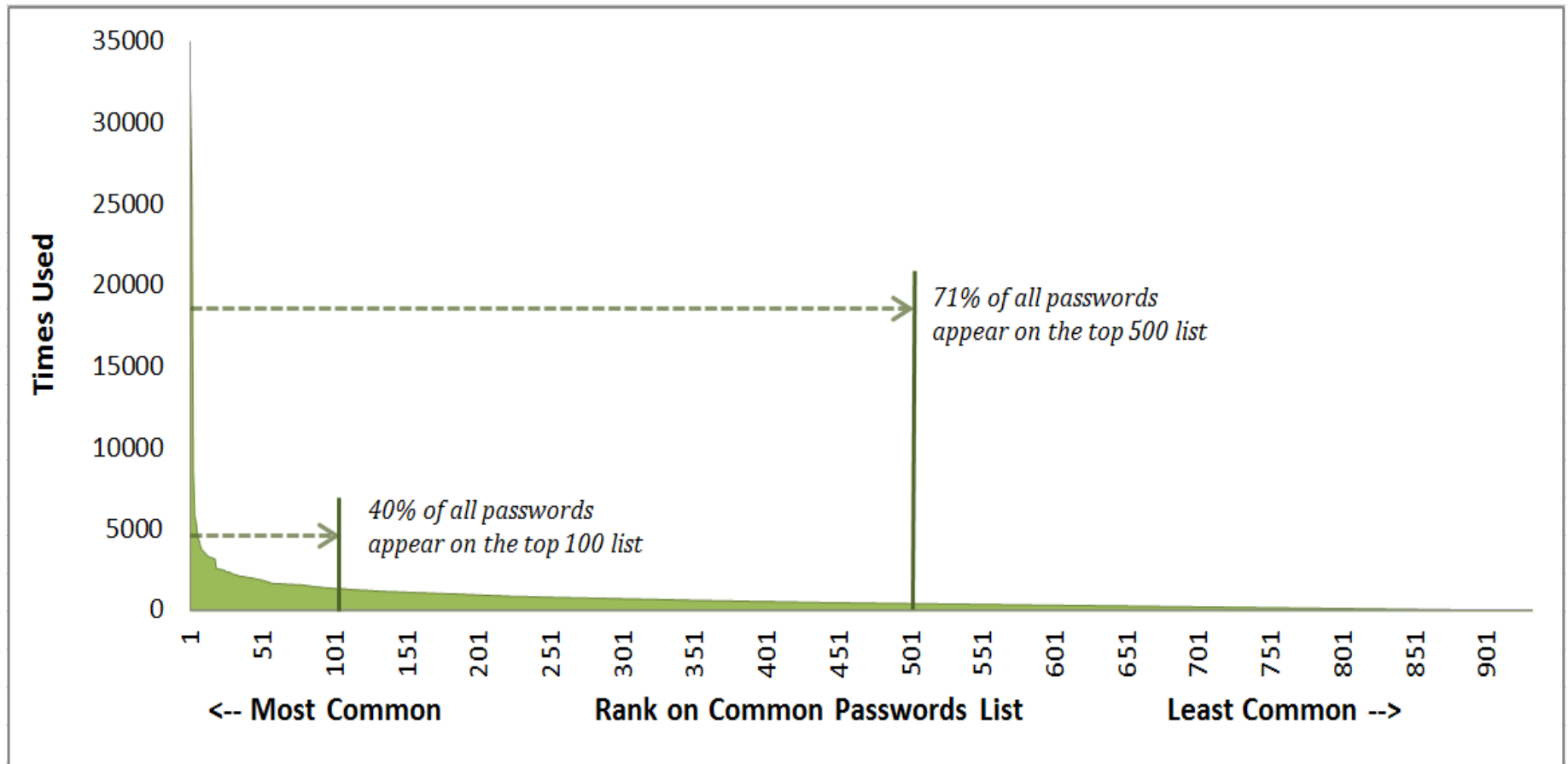
Dictionary Attacks



- One of the simplest forms of a guessing attack is a dictionary attack
- Dictionary attacks use a word list as the input to the guess attempts
 - The more words, the more guesses
 - However, if the password is not in the dictionary, a match will not be found
 - May not yield a result
 - These word lists are readily available and often based on leaked passwords
 - Have lists with top 500, 10k, 1M, and 50M password guesses
- These dictionaries can also be weighted based on likelihood of usage
 - Most common passwords first to allow routines to “short circuit” once match is found
- Allow simple modifications to dictionary words
 - Change case, all lower, all upper, first Upper character only
 - Append digit(s) or special characters to end
 - Use of “leetspeak” substitutions – 1 for l or L, 3 for E, 4 for A, 8 for B, \$ for S
- Can use a method known as “spidering” to specialized targets
 - Custom dictionaries based on business, brand, sector, industry, location, geography



How Big of Dictionary Do You Need?



- Based on 6 Million leaked passwords
 - 40% in top 100 passwords
 - 71% in top 500 passwords

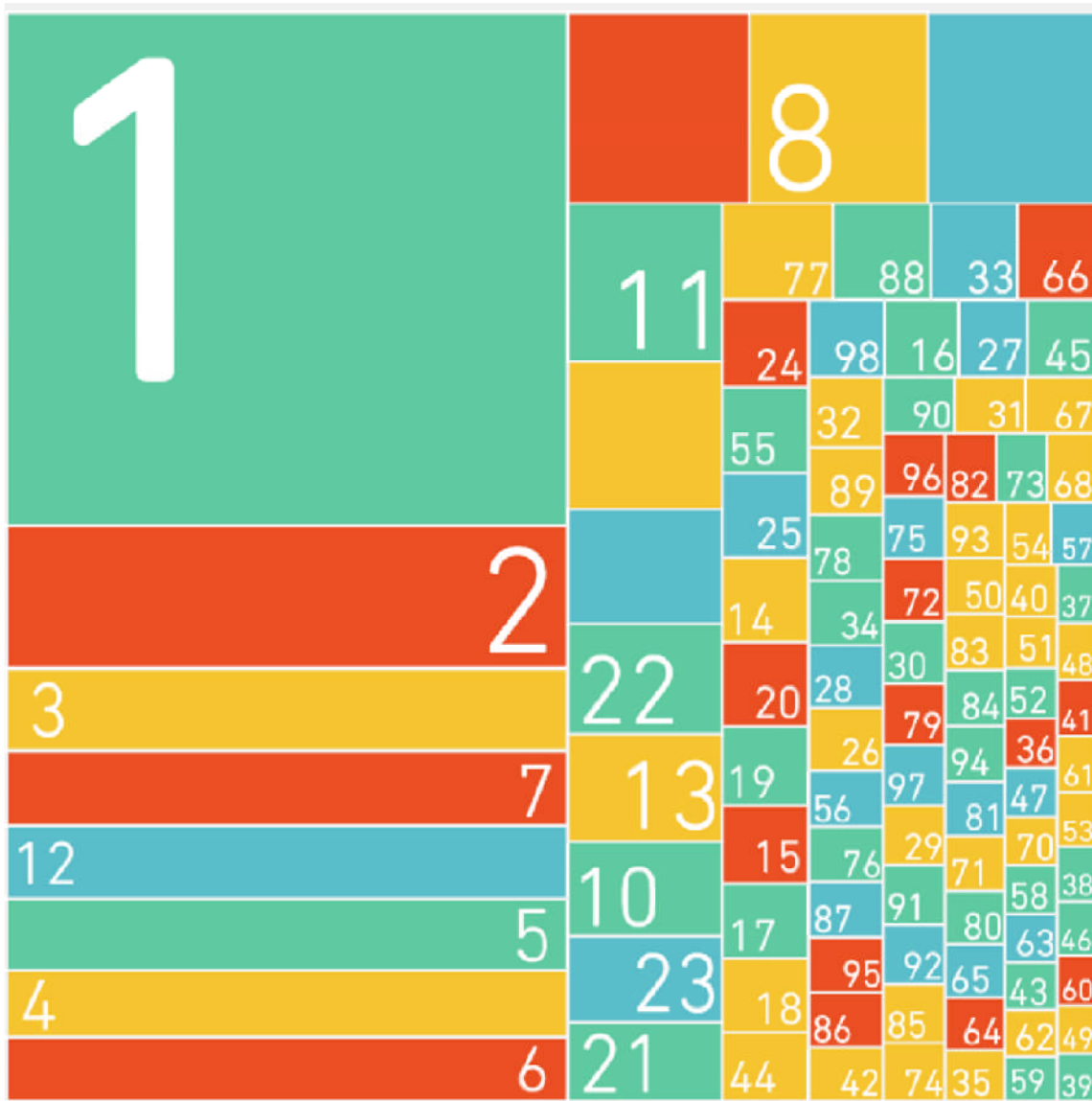
Source:
Mark Burnett,
<https://xato.net/>

50 Most Used Passwords

1. 123456
2. password
3. 12345678
4. qwerty
5. 123456789
6. 12345
7. 1234
8. 111111
9. 1234567
10. dragon
11. 123123
12. baseball
13. abc123
14. football
15. monkey
16. letmein
17. shadow
18. master
19. 696969
20. michael
21. mustang
22. 666666
23. qwertyuiop
24. 123321
25. 1234...890
26. p*s*y
27. superman
28. 270
29. 654321
30. 1qaz2wsx
31. 7777777
32. f*cky*u
33. qazwsx
34. jordan
35. jennifer
36. 123qwe
37. 121212
38. killer
39. trustno1
40. hunter
41. harley
42. zxcvbnm
43. asdfgh
44. buster
45. andrew
46. batman
47. soccer
48. tigger
49. charlie
50. robert

Source:
WP Engine
Unmasked

Adding a Number to the End



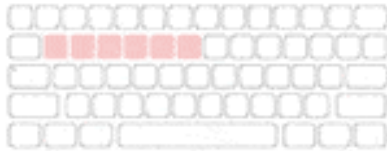
Most Used Numbers (0-99) at the End of Passwords

1. **examplepassword1** 23.84%
2. **examplepassword2** 6.72%
3. **examplepassword3** 3.86%
4. **examplepassword12** 3.55%
5. **examplepassword7** 3.54%
6. **examplepassword5** 3.35%
7. **examplepassword4** 3.19%
8. **examplepassword6** 3.06%
9. **examplepassword9** 2.91%
10. **examplepassword8** 2.89%

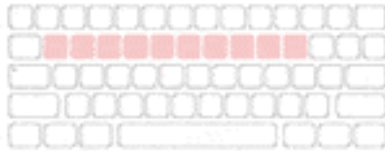
Source:
WP Engine
Unmasked

Pattern Passwords

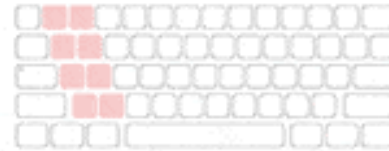
① qwerty



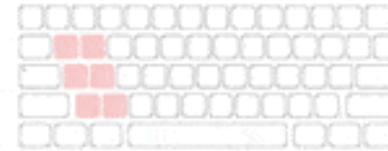
② qwertyuiop



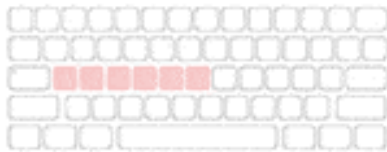
③ 1qaz2wsx



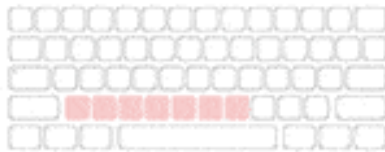
④ qazwsx



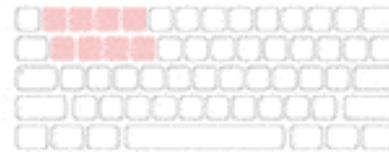
⑤ asdfgh



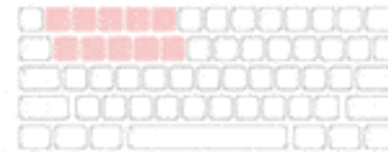
⑥ zxcvbnm



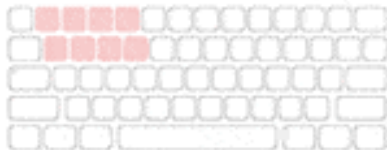
⑦ 1234qwer



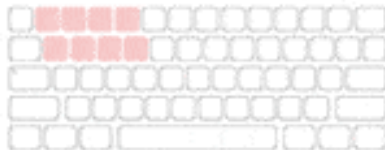
⑧ q1w2e3r4t5



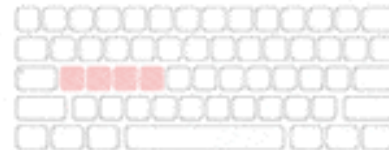
⑨ qwer1234



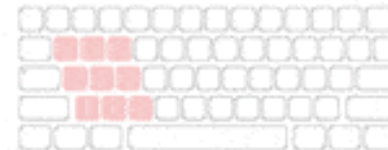
⑩ q1w2e3r4



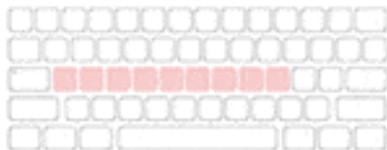
⑪ asdfasdf



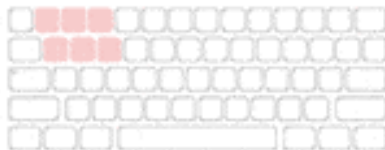
⑫ qazwsxedc



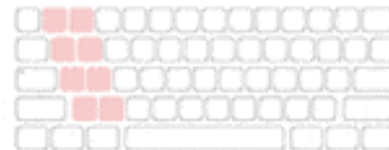
⑬ asdfghjkl



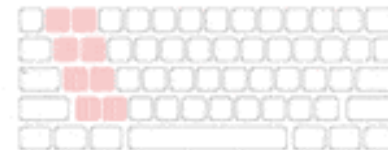
⑭ q1w2e3



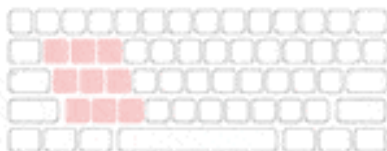
⑮ 1qazxsw2



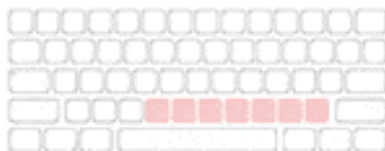
⑯ 12QWaszx



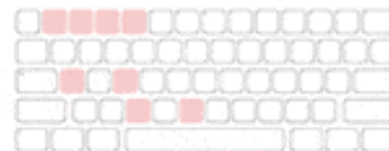
⑰ qweasdzc



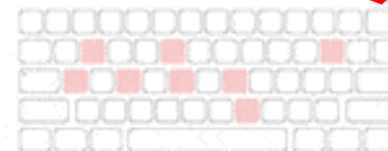
⑱ mnbcvxz



⑲ a1b2c3d4

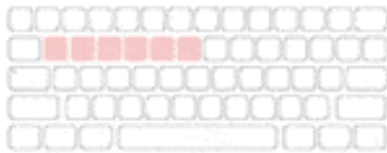


⑳ adgjmntw

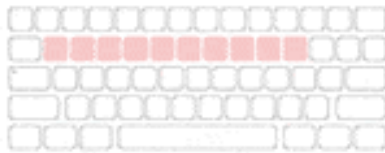


Pattern Passwords

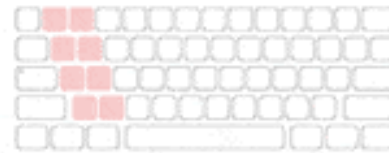
① qwerty



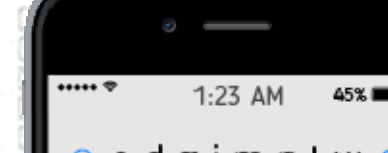
② qwertyuiop



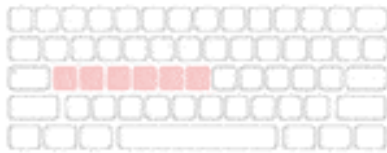
③ 1qaz2wsx



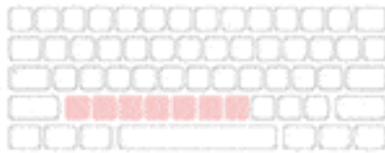
④ nazwsx



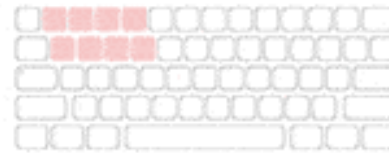
⑤ asdfgh



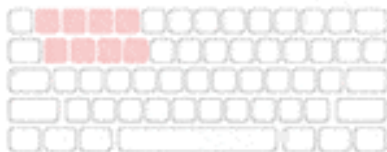
⑥ zxcvbnm



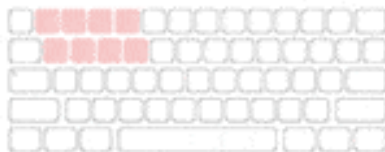
⑦ 1234qwer



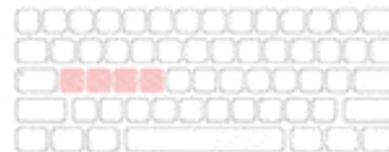
⑨ qwer1234



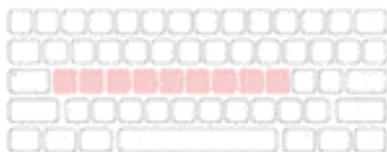
⑩ q1w2e3r4



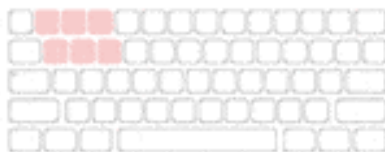
⑪ asdfasdf



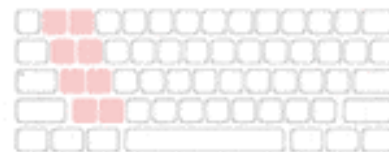
⑬ asdfghjkl



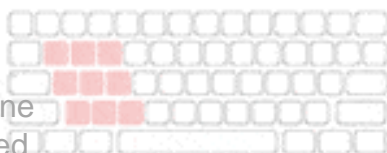
⑭ q1w2e3



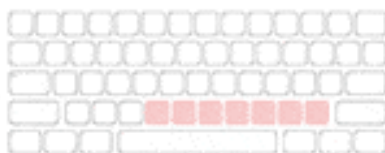
⑮ 1qazxsw2



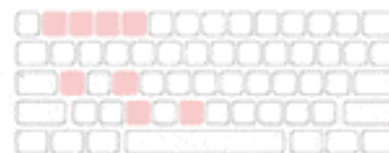
⑰ qweasdzc



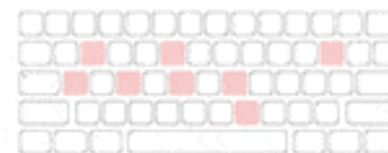
⑱ mnbcvxz



⑲ a1b2c3d4

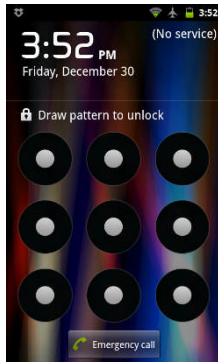


⑳ adgj mptw



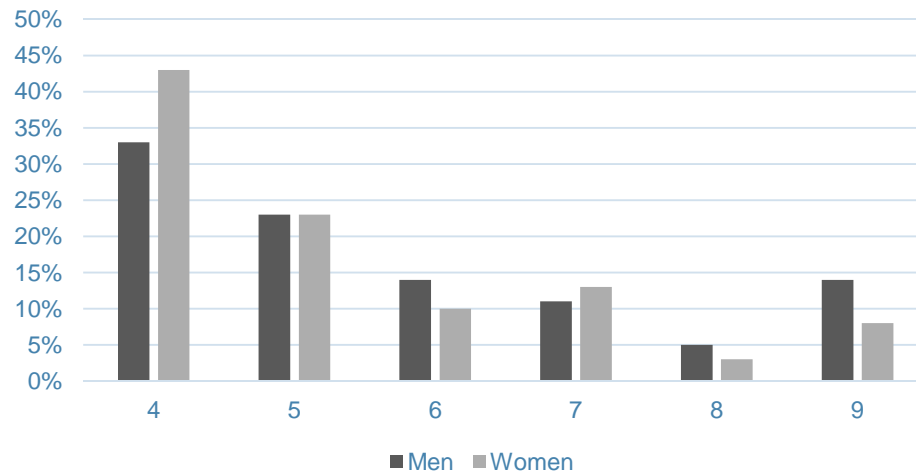
Source:
WP Engine
Unmasked

Android Lock Patterns (ALP)

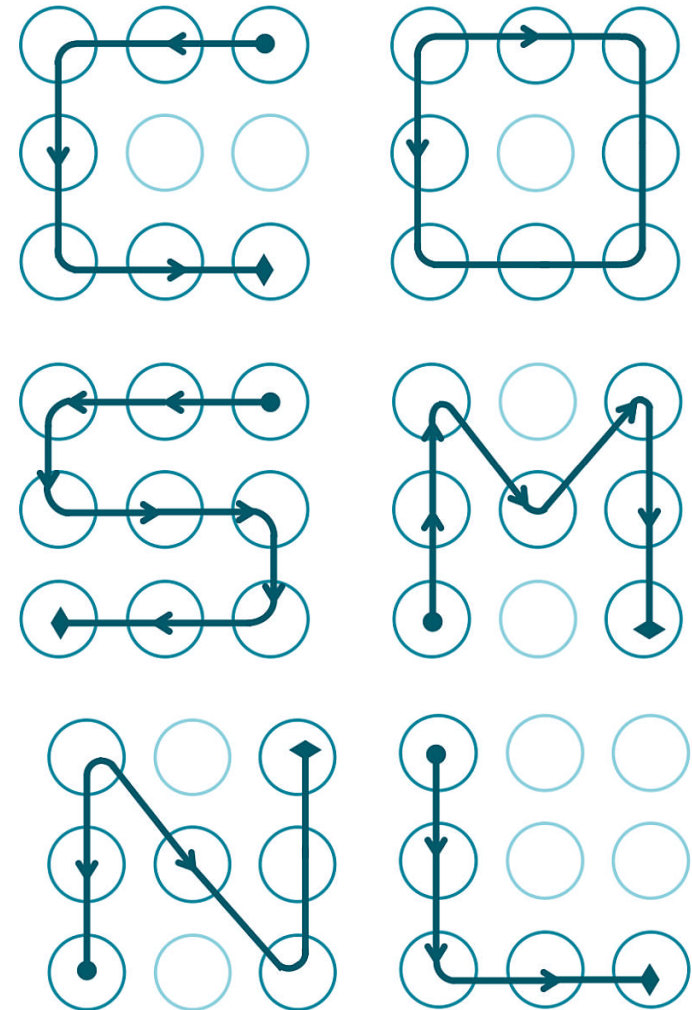


Nodes	Possible Combinations
4	1,624
5	7,152
6	26,016
7	72,912
8	140,704
9	140,704

Number of Nodes in ALP



Men	33%	23%	14%	11%	5%	14%
Women	43%	23%	10%	13%	3%	8%
Nodes	4	5	6	7	8	9



Dictionary Attack Considerations

- Pros:
 - Can run very fast with a limited set of possible guesses
 - Uses people's desire for a simple, easy to remember password against them
 - If rules are not in place, good chance of matching result
 - Also useful to catch administrators which often have rights to set passwords that do not follow the rules in place for the general users (At IBM i 7.2, can set QPWDRULES system value to include *ALLCRTCHG to prevent this!)
 - These accounts are often privileged users with higher access rights!
 - Admins are lazy too! Can be used against them!!
- Cons:
 - May not find a match and time attempted is wasted
 - Time it may take to customize a dictionary
 - Password rules such as case, digit, and special character requirements dramatically limit the effectiveness of a dictionary attack
 - Length requirements reduce effectiveness





JUST BRUTAL....

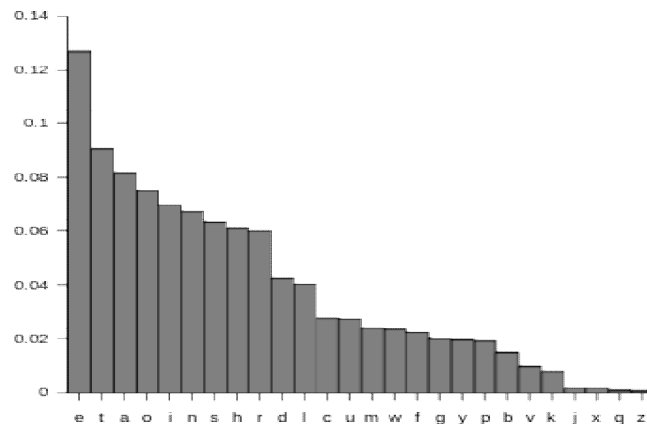
Brute Force Attacks



Brute Force Attacks



- Try all possible combinations of the character set as the guess to find a matching value
 - Imagine an old style analog odometer, but with characters as well as numbers
 - A, AB, ABC, AA, BB, CC, AAB, AAC, BBB, CCC, etc.....
 - Given enough time it will find the correct value!!
 - Quickly becomes time consuming the longer the possible password is
 - Resources required for attack grow exponentially to password length, not linearly
 - Average result is expected in: Total Attempts Possible / 2
 - Total Number of attempts required: (size of character set) ^ (password length)
- Can re-order the alphabet used based on English language or prior cracked password frequency tables to attempt to locate the password sooner
 - ETAOI12NSH0RD3QZL45CU96MWFG87YPBVKJX\$@#_



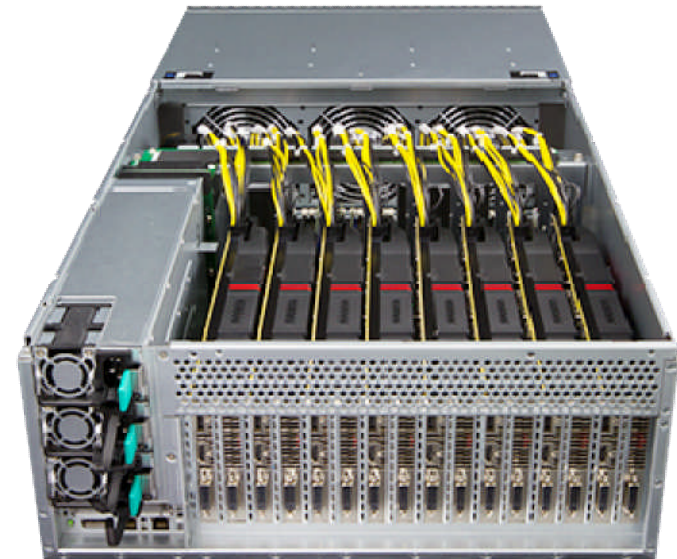
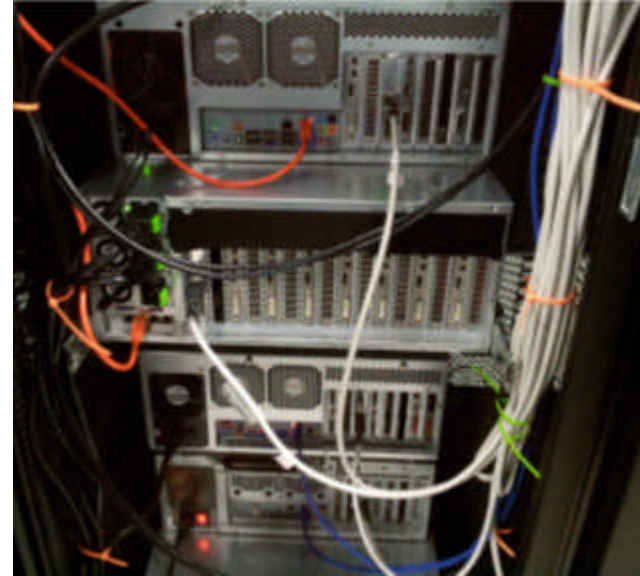
Overall Character Frequency Charset:
aeorisn1tl2md0cp3hbuk45g9687yfwjvzxq

First Character Frequency Charset:
s1mpabctdrflfhgkjinw2ei0ov3q45796z8yux

Last Character Frequency Charset:
e1nsra326yt0d954o78lkgmihbpcxuwfzjvq

Brute Force Estimates

- Hardware: 5 x 4U servers, 25 GPUs, Infiniband 10G networking
 - Price estimate: \$20,000
 - Speed:
 - Password Level 0/1: 180,000,000,000/second
 - Password Level 2/3: 63,000,000,000/second
- Time to Crack:
 - IBM i Password Level 0/1 – 40 Characters
 - 4 long: 1.86 Million (sub-second)
 - 6 long: 2.97 Billion (sub-second)
 - 8 long: 4.75 Trillion (26.4 seconds)
 - 10 long: 7.6 Quadrillion (11.7 hours)
 - IBM i Password Level 2/3 – 95 Characters
 - 4 long: 80.59 Million (sub-second)
 - 6 long: 727.4 Billion (11.5 seconds)
 - 8 long: 6.56 Quadrillion (28.9 hours)
 - 10 long: 59.2 Quintillion (Months)



COTS Hardware!

GPU Compute Nodes

Sagitta HPC offers three different models of GPU compute nodes to scale to your precise needs. From small penetration testing teams to large government organizations, Sagitta offers state-of-the-art GPU compute nodes that accelerate password cracking workloads, improve efficiency, and extend the capabilities of your team. With a solution for every budget and requirement, Sagitta HPC makes it easy to take advantage of the latest advances in high performance password cracking.



Brutalis

Brutalis is an eight-GPU monster, clawing its way through hashes at unprecedented speeds. Providing up to eight AMD or Nvidia GPUs,



Invictus

Invictus is a quad-GPU system for password cracking professionals with medium-size workloads and large expectations. Providing up to



Inceptus

Inceptus is a three-GPU system perfect for novice crackers and professionals on a budget. Providing up to three AMD or

State of Passwords Today

<p>UNCOMMON (NON-GIBBERISH) BASE WORD</p> <p>ORDER UNKNOWN</p> <p>Tr0ub4dor &3</p> <p>CAPS? COMMON SUBSTITUTIONS NUMERAL PUNCTUATION</p> <p>(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)</p>	<p>~28 BITS OF ENTROPY</p> <p>$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$</p> <p>(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)</p> <p>DIFFICULTY TO GUESS: EASY</p>	<p>WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?</p> <p>AND THERE WAS SOME SYMBOL...</p> <p>DIFFICULTY TO REMEMBER: HARD</p>
<p>correct horse battery staple</p> <p>FOUR RANDOM COMMON WORDS</p>	<p>~44 BITS OF ENTROPY</p> <p>$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$</p> <p>DIFFICULTY TO GUESS: HARD</p>	<p>THAT'S A BATTERY STAPLE.</p> <p>CORRECT!</p> <p>DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT</p>

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Password Rules Affect on Password Levels 0/1

		Password Length										
		1	2	3	4	5	6	7	8	9	10	
P a s s w o r d R u l e s	None	29	1,160	46,400	1,856,000	74,240,000	2,969,600,000	118,784,000,000	4,751,360,000,000	190,054,400,000,000	7,602,176,000,000,000	
	*CHRLMTAJC Limit 2 same chars adjacent	29	1,131	44,109	1,720,251	67,089,789	2,616,501,771	102,043,569,069	3,979,699,193,691	155,208,268,553,949	6,053,122,473,604,010	
		Strength compared to none	100.00%	97.50%	95.06%	92.69%	90.37%	88.11%	85.91%	83.76%	81.67%	79.62%
	*CHRLMTREP Limit 2 same chars anywhere	29	1,131	42,978	1,590,186	57,246,696	2,003,634,360	68,123,568,240	2,248,077,751,920	71,938,488,061,440	2,230,093,129,904,640	
		Strength compared to none	100.00%	97.50%	92.63%	85.68%	77.11%	67.47%	57.35%	47.31%	37.85%	29.33%
	*DGLMTFST First not digit *	29	1,160	46,400	1,856,000	74,240,000	2,969,600,000	118,784,000,000	4,751,360,000,000	190,054,400,000,000	7,602,176,000,000,000	
		Strength compared to none	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
	*DGLMTLST Last not digit	29	870	34,800	1,392,000	55,680,000	2,227,200,000	89,088,000,000	3,563,520,000,000	142,540,800,000,000	5,701,632,000,000,000	
		Strength compared to none	100.00%	75.00%	75.00%	75.00%	75.00%	75.00%	75.00%	75.00%	75.00%	75.00%
	*DGTMIN1 At least 1 digit	N/A	290	11,600	464,000	18,560,000	742,400,000	29,696,000,000	1,187,840,000,000	47,513,600,000,000	1,900,544,000,000,000	
		Strength compared to none	N/A	25.00%	25.00%	25.00%	25.00%	25.00%	25.00%	25.00%	25.00%	25.00%
	*LTRLMTFST First not letter	3	120	4,800	192,000	7,680,000	307,200,000	12,288,000,000	491,520,000,000	19,660,800,000,000	786,432,000,000,000	
		Strength compared to none	10.34%	10.34%	10.34%	10.34%	10.34%	10.34%	10.34%	10.34%	10.34%	10.34%
	*LTRLMTLST Last not letter	3	406	16,240	649,600	25,984,000	1,039,360,000	41,574,400,000	1,662,976,000,000	66,519,040,000,000	2,660,761,600,000,000	
		Strength compared to none	10.34%	35.00%	35.00%	35.00%	35.00%	35.00%	35.00%	35.00%	35.00%	35.00%
	*SPCCHRLMTFST First not special char	26	1,040	41,600	1,664,000	66,560,000	2,662,400,000	106,496,000,000	4,259,840,000,000	170,393,600,000,000	6,815,744,000,000,000	
		Strength compared to none	89.66%	89.66%	89.66%	89.66%	89.66%	89.66%	89.66%	89.66%	89.66%	89.66%
	*SPCCHRLMTLST Last not special char	26	936	37,440	1,497,600	59,904,000	2,396,160,000	95,846,400,000	3,833,856,000,000	153,354,240,000,000	6,134,169,600,000,000	
		Strength compared to none	89.66%	80.69%	80.69%	80.69%	80.69%	80.69%	80.69%	80.69%	80.69%	80.69%
	*SPCCHRMIN1 At least 1 special char	3	116	4,640	185,600	7,424,000	296,960,000	11,878,400,000	475,136,000,000	19,005,440,000,000	760,217,600,000,000	
	Strength compared to none	10.34%	10.00%	10.00%	10.00%	10.00%	10.00%	10.00%	10.00%	10.00%	10.00%	
*DGTMIN1, *LTRMIN1, *SPCCHARMIN1	N/A	N/A	1,040	41,600	1,664,000	66,560,000	2,662,400,000	106,496,000,000	4,259,840,000,000	170,393,600,000,000		
	Strength compared to none	N/A	N/A	2.24%	2.24%	2.24%	2.24%	2.24%	2.24%	2.24%	2.24%	

Password Rules Affect on Password Levels 2/3

Password Length

		1	2	3	4	5	6	7	8	9	10
None		94	8,930	848,350	80,593,250	7,656,358,750	727,354,081,250	69,098,637,718,750	6,564,370,583,281,250	623,615,205,411,719,000	59,243,444,514,113,300,000
*CHRLMTAJC	Limit 2 same chars adjacent	94	8,836	830,584	78,074,896	7,339,040,224	689,869,781,056	64,847,759,419,264	6,095,689,385,410,820	572,994,802,228,617,000	53,861,511,409,490,000,000
	Strength compared to none	100.00%	98.95%	97.91%	96.88%	95.86%	94.85%	93.85%	92.86%	91.88%	90.92%
*CHRLMTREP	Limit 2 same chars anywhere	94	8,836	821,748	75,600,816	6,879,674,256	619,170,683,040	55,106,190,790,560	4,849,344,789,569,280	421,892,996,692,527,000	36,282,797,715,557,400,000
	Strength compared to none	100.00%	98.95%	96.86%	93.81%	89.86%	85.13%	79.75%	73.87%	67.65%	61.24%
*DGLMTFST	First not digit	84	7,980	758,100	72,019,500	6,841,852,500	649,975,987,500	61,747,718,812,500	5,866,033,287,187,500	557,273,162,282,812,000	52,940,950,416,867,200,000
	Strength compared to none	89.36%	89.36%	89.36%	89.36%	89.36%	89.36%	89.36%	89.36%	89.36%	89.36%
*DGLMTLST	Last not digit	84	7,990	759,050	72,109,750	6,850,426,250	650,790,493,750	61,825,096,906,250	5,873,384,206,093,750	557,971,499,578,906,000	53,007,292,459,996,100,000
	Strength compared to none	89.36%	89.47%	89.47%	89.47%	89.47%	89.47%	89.47%	89.47%	89.47%	89.47%
*DGTMIN1	At least 1 digit	10	950	90,250	8,573,750	814,506,250	77,378,093,750	7,350,918,906,250	698,337,296,093,750	66,342,043,128,906,200	6,302,494,097,246,090,000
	Strength compared to none	10.64%	10.64%	10.64%	10.64%	10.64%	10.64%	10.64%	10.64%	10.64%	10.64%
*LTRLMTFST	First not letter	42	3,990	379,050	36,009,750	3,420,926,250	324,987,993,750	30,873,859,406,250	2,933,016,643,593,750	278,636,581,141,406,000	26,470,475,208,433,600,000
	Strength compared to none	44.68%	44.68%	44.68%	44.68%	44.68%	44.68%	44.68%	44.68%	44.68%	44.68%
*LTRLMTLST	Last not letter	42	4,042	383,990	36,479,050	3,465,509,750	329,223,426,250	31,276,225,493,750	2,971,241,421,906,250	282,267,935,081,094,000	26,815,453,832,703,900,000
	Strength compared to none	44.68%	45.26%	45.26%	45.26%	45.26%	45.26%	45.26%	45.26%	45.26%	45.26%
*SPCCHRLMTFST	First not special char	62	5,890	559,550	53,157,250	5,049,938,750	479,744,181,250	45,575,697,218,750	4,329,691,235,781,250	411,320,667,399,219,000	39,075,463,402,925,800,000
	Strength compared to none	65.96%	65.96%	65.96%	65.96%	65.96%	65.96%	65.96%	65.96%	65.96%	65.96%
*SPCCHRLMTLST	Last not special char	62	5,828	553,660	52,597,700	4,996,781,500	474,694,242,500	45,095,953,037,500	4,284,115,538,562,500	406,990,976,163,438,000	38,664,142,735,526,600,000
	Strength compared to none	65.96%	65.26%	65.26%	65.26%	65.26%	65.26%	65.26%	65.26%	65.26%	65.26%
*SPCCHRMIN1	At least 1 special char	32	3,102	294,690	27,995,550	2,659,577,250	252,659,838,750	24,002,684,681,250	2,280,255,044,718,750	216,624,229,248,281,000	20,579,301,778,586,700,000
	Strength compared to none	34.04%	34.74%	34.74%	34.74%	34.74%	34.74%	34.74%	34.74%	34.74%	34.74%
*DGTMIN1, *LTRMIN1, *SPCCHARMIN1		N/A	N/A	17,160	1,630,200	154,869,000	14,712,555,000	1,397,692,725,000	132,780,808,875,000	12,614,176,843,125,000	1,198,346,800,096,880,000
	Strength compared to none	N/A	N/A	2.02%	2.02%	2.02%	2.02%	2.02%	2.02%	2.02%	2.02%

Brute Force Considerations

- Pros:

- Will always find the password, given enough time and resources
- Password rules such as case, digit, and special character requirements dramatically increase the effectiveness of a brute force attack by eliminating possible passwords that do not match the rule set
 - The more complex the rules, the less possible values to test!

- Cons:

- Minimum length requirements highly reduce effectiveness
- Password may be changed before result is found
- May take a very long time to run





AND WHY THE IBM I IS SAFE... OR CAN BE MADE SAFE! ARE YOU?

Other Attacks



Other Attacks (and Their Foes)

- Rainbow tables
 - Use pre-computed tables to save time by looking up values instead of calculating them
 - Only viable with hash method is static and without “salt” (random crypto value)
 - Adding salt defeats rainbow tables
- Phishing/Social Engineering
 - Attempts to pose as someone else to gain access to passwords
 - Education is best way to defeat phishing and social engineering
- Key Logger
 - Software or hardware that records everything typed on keyboards
 - Virtual keyboards, patterns, and non-typed passwords defeat key loggers
- Network Sniffing
 - Recording everything transmitted over the network (private and/or public Internet)
 - Encrypting everything from client to server defeats network sniffing
- Shoulder Surfing
 - Having keyboard or screen watched by someone else
 - Education and screen privacy filters help defeat shoulder surfing



Example of Shoulder Surfing



"You spelled 'confidential' wrong."



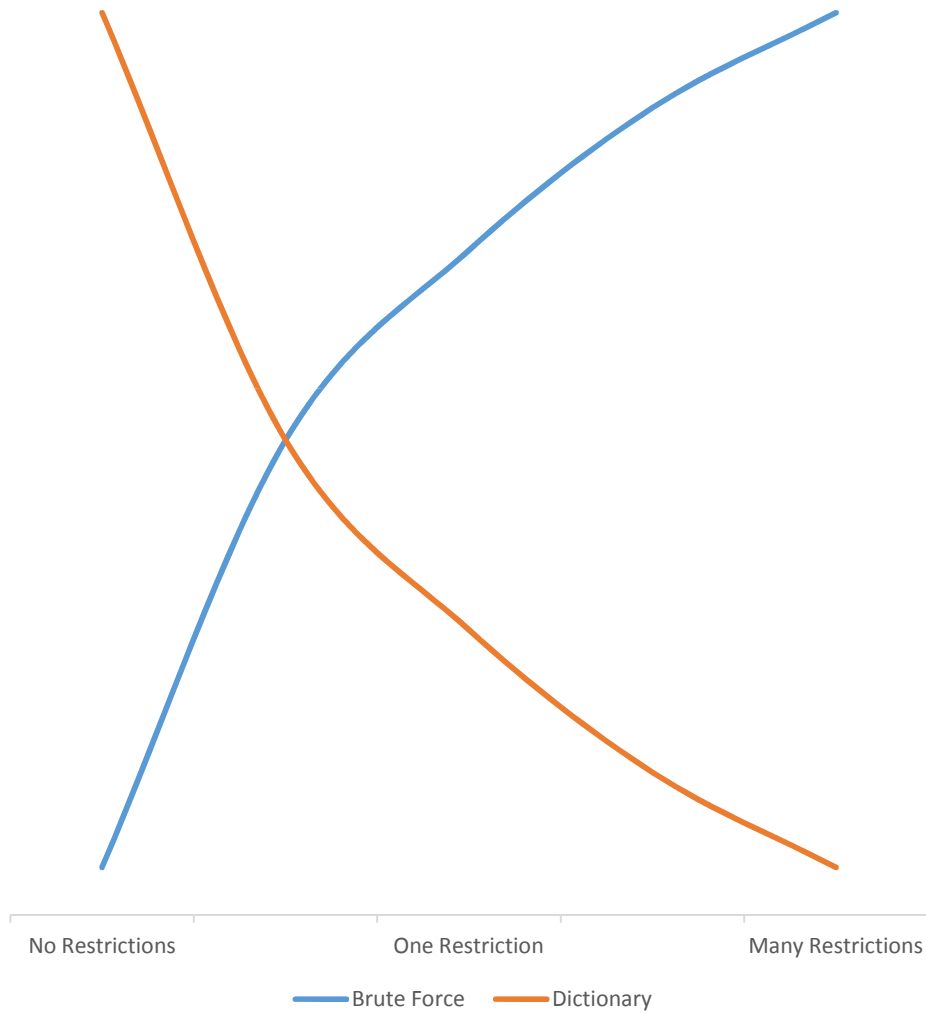
THE FUTURE OF PASSWORDS

Putting it All Together

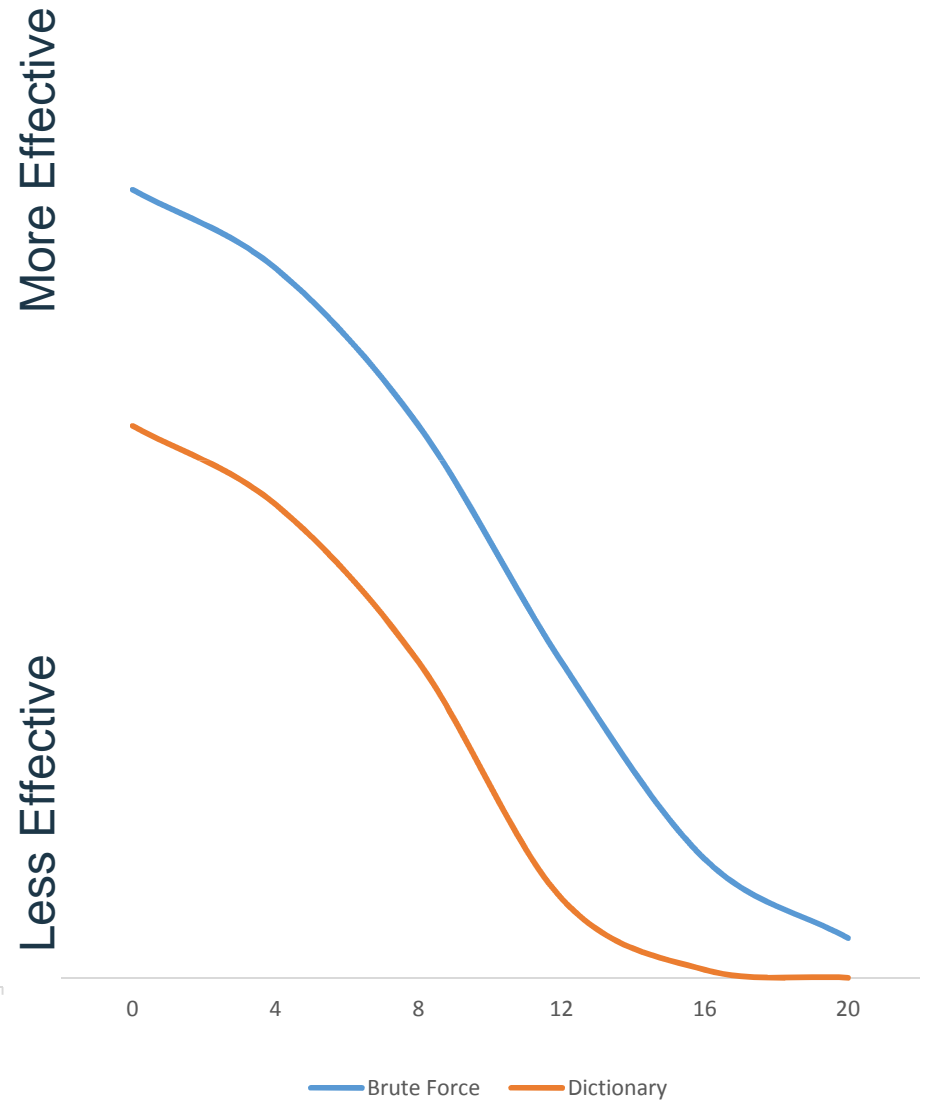


Attack Effectiveness vs. Password Characteristics

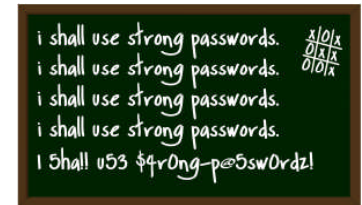
Attack Effectiveness vs. Password Restrictions



Attack Effectiveness vs. Password Length



Password Length



- Our best defense today is to require longer passwords, or pass phrases using a full character set of 95 possible values (Password Level 3)
- Longer does not need to be more complex to remember
 - Rather than complex short passwords, use a string or phrase that is easy to remember
- Can also employ a concept known as “password haystacks” or password padding
 - Take a simple to remember but short password – Example: Gr33nTr33s
 - Pad it with a simple special character pattern – Example: ..
 - Thus increasing its length Example:Gr33nTr33s.....
 - We have gone from 10 long to 22
 - Thus this is 540,360,087,662,636,962,890,625 times more secure!!
- Which of the following two passwords is stronger, more secure, and more difficult to crack?
 - D0g.....
 - PrXyc.N(n4k77#L!eVdAfp9

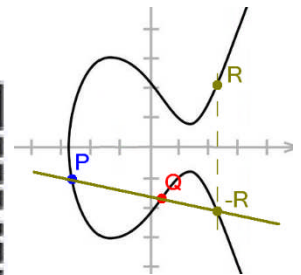
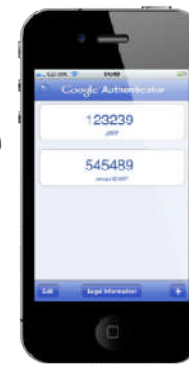
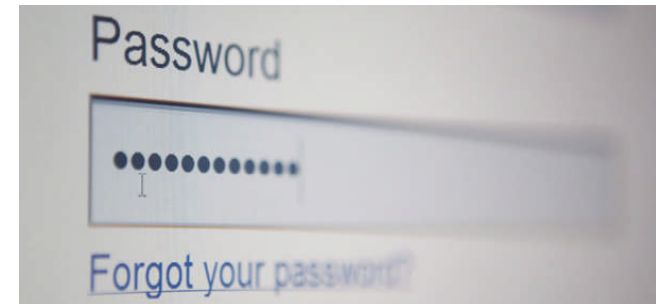
TIME TO CRACK:

35,000,000,000,000,000,000,000
YEARS

Compl3xity < Length!

Where Do We Go From Here?

- The current state of passwords, while once considered safe, are quickly becoming unsafe
- There are newer methods and options that exist
- However adoption of these items has been glacially slow
 - Second/multi factor and biometrics
 - Password vaults and random password generation
 - Zero knowledge proof single use passwords
 - No shared secret methodologies
 - Out of band authentication
 - Strong Single Sign On
- Until then, length of passwords is our best protection



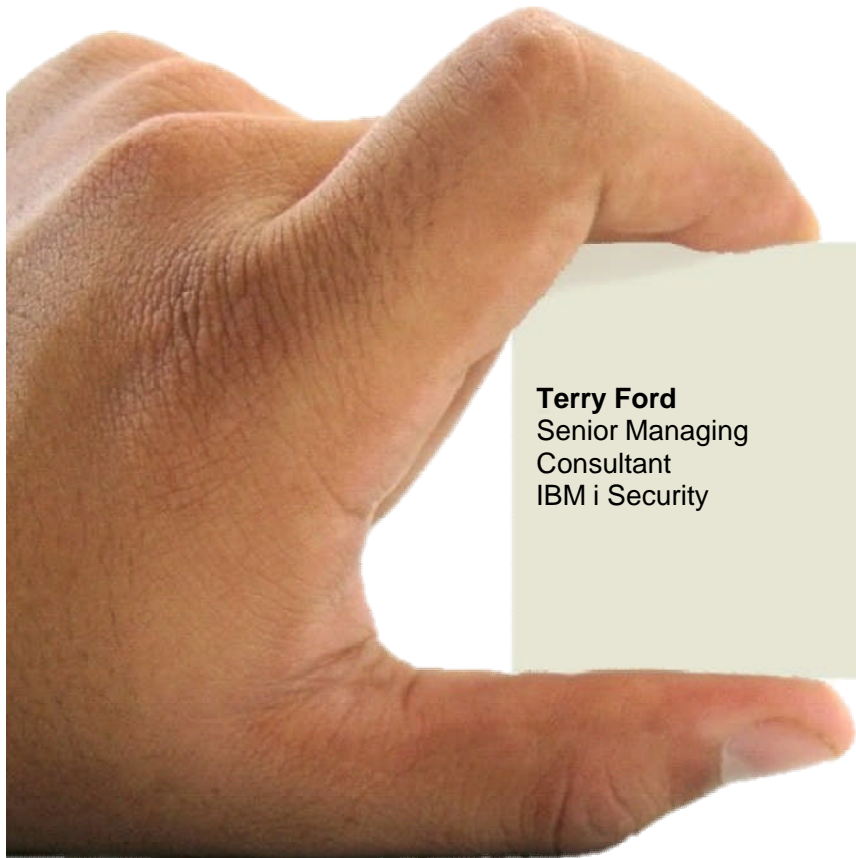
IBM Lab Services Can Help!



- IBM Lab Services can offer consulting and security services:
 - IBM i Security Assessment
 - IBM i Network Encryption (TLS)
 - IBM i Single Sign On Setup

- IBM Lab Services also has several security related tools:
 - IBM i Software Firewall (Exit Points)
 - IBM i Privileged Elevation Tool (FireCall)
 - IBM i Compliance and Reporting Tool with Event Monitoring
 - IBM i Two Factor Authentication / Password Reset Utility
 - And many more non-network related tools

- Visit <http://ibm.biz/IBMiSecurity> to learn more about all of these offerings!



IBM

Terry Ford
Senior Managing
Consultant
IBM i Security

Office: 1-507-253-7241
Mobile: 1-507-358-1771
taford@us.ibm.com

3605 Highway 52 N
Bldg. 025-3 C113
Rochester, MN 55901
USA






THANK YOU

FOLLOW US ON:

 ibm.biz/IBMiSecurity

 ibm.com/systems/services/labservices

 [@ibmsecurity](https://twitter.com/ibmsecurity)

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.





Notices and Disclaimers

Copyright © 2016 by International Business Machines Corporation (IBM). No part of this document may be reproduced or transmitted in any form without written permission from IBM.

U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IN NO EVENT SHALL IBM BE LIABLE FOR ANY DAMAGE ARISING FROM THE USE OF THIS INFORMATION, INCLUDING BUT NOT LIMITED TO, LOSS OF DATA, BUSINESS INTERRUPTION, LOSS OF PROFIT OR LOSS OF OPPORTUNITY. IBM products and services are warranted according to the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. IBM EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, ibm.com, Aspera®, Bluemix, Blueworks Live, CICS, Clearcase, Cognos®, DOORS®, Emptoris®, Enterprise Document Management System™, FASP®, FileNet®, Global Business Services®, Global Technology Services®, IBM ExperienceOne™, IBM SmartCloud®, IBM Social Business®, Information on Demand, ILOG, Maximo®, MQIntegrator®, MQSeries®, Netcool®, OMEGAMON, OpenPower, PureAnalytics™, PureApplication®, pureCluster™, PureCoverage®, PureData®, PureExperience®, PureFlex®, pureQuery®, pureScale®, PureSystems®, QRadar®, Rational®, Rhapsody®, Smarter Commerce®, SoDA, SPSS, Sterling Commerce®, StoredIQ, Tealeaf®, Tivoli®, Trusteer®, Unica®, urban{code}®, Watson, WebSphere®, Worklight®, X-Force® and System z® Z/OS, are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.

