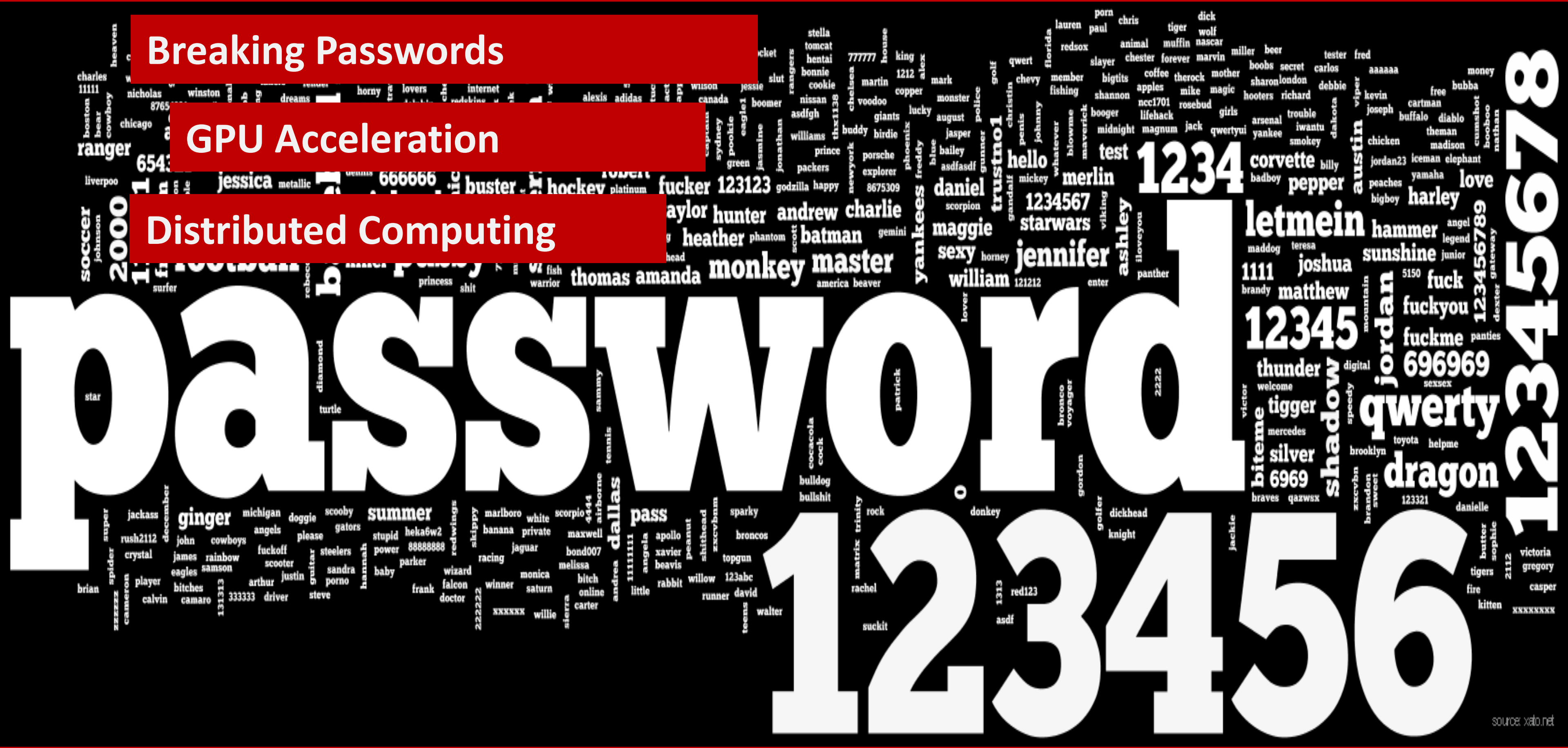
Breaking Passwords and Overcoming Encryption

Breaking Passwords

Recovering encrypted evidence and accessing password-protected data

Breaking Passwords



- Breaking Passwords
- GPU Acceleration
- Distributed Computing

Types of Protection

- **Password locks access**
  - Instant recovery possible
- **Weak encryption**
  - Instant recovery with Thunder Tables
- **Strong encryption**: passwords must be enumerated
  - List of common passwords
  - Smart dictionary attacks and mutations
  - GPU acceleration
  - Zero-overhead distributed computing

Some Passwords are Weaker Than Others

Instant Password Recovery

- Microsoft Office up to XP/2003
- Intuit Quicken (old versions)
- Intuit QuickBooks
- Adobe Acrobat PDF (protection passwords)
- Microsoft Office (protection passwords)
- Browsers: IE, Edge, Firefox, Opera, Safari, Chrome
- Instant messengers (over 80)
- Mail clients (over 15)
- Windows logon passwords
- Microsoft SQL
- Sage products (ACT!, PeachTree Accounting)
- Lotus Smart Suite
- WordPerfect Office

Some Passwords are Weaker Than Others

Quickly Recoverable >500,000 p/s

- Windows LM and NTLM
- MD5, sha1,sha256,sha512
- Microsoft SQL Server, SQL CE
- PFX/P12 certificates
- macOS keychain
- ZIP archives (classic encryption)
- iOS 10.0 backups

Some Passwords are Just Normal

Around 50,000 to 100,000 p/s

- WPA/WPA2 PSK
- IBM Notes (some versions)
- ZIP (AES)
- iTines backups (iOS 4-9, 10.1)
- Microsoft Office 2007/2010
- Hancell

Some Passwords are Stronger Than Others

Slower than 50,000 p/s

- Microsoft Office 2013/2016
- RAR and 7zip archives
- macOS logon password
- TrueCrypt, FileVault2, BitLocker
- iOS 10.2+ backups

Some Passwords are Stronger Than Others

Varies depending on version/algorithm

- OpenOffice
- IBM/Lotus Notes
- PGP
- Domain Cached Credentials
- Password managers

MS Office 2007 / 2010 / 2013

CPU: Intel Xeon E5-2603
GPU: AMD Radeon R9 290

One instance

	Per second	Per hour
MS Office 2007	46.200	166.320.000
MS Office 2010	24.500	88.200.000
MS Office 2013	2.900	1.044.000

MS Office 2007 / 2010 / 2013

CPU: Intel Xeon E5-2603
GPU: AMD Radeon R9 290

10 instances

	Per second	Per hour
MS Office 2007	462.000	1.663.200.000
MS Office 2010	245.000	882.000.000
MS Office 2013	29.000	10.440.000

MS Office 2007 / 2010 / 2013

10 instances

Is brute-force enough to break passwords in reasonable time?

	Per second	Per hour
MS Office 2007	462.000	1.663.200.000
MS Office 2010	245.000	882.000.000
MS Office 2013	29.000	10.440.000

MS Office 2013

Very simple: 5 characters (lower case letters and numbers only)

36^5= 60,466,176 possible passwords

Max. time: **4.7 hours**

MS Office 2013

Simple: 6 characters (lower and upper case letters and numbers only)

62^6= 56,800,235,584 possible passwords

Max. time: **4500 hours (6 months)**

MS Office 2013

Average: 7 characters (upper and lower case letters and numbers)

62^7= 3,521,614,606,208 possible passwords

Max. time:

MS Office 2013

Average: 7 characters (upper and lower case letters and numbers)

62^7= 3,521,614,606,208 possible passwords

Max. time: **277.292 hours (31.5 years)**

MS Office 2013

Slightly stronger than average: 8 characters (upper and lower case letters, special characters and numbers combined)

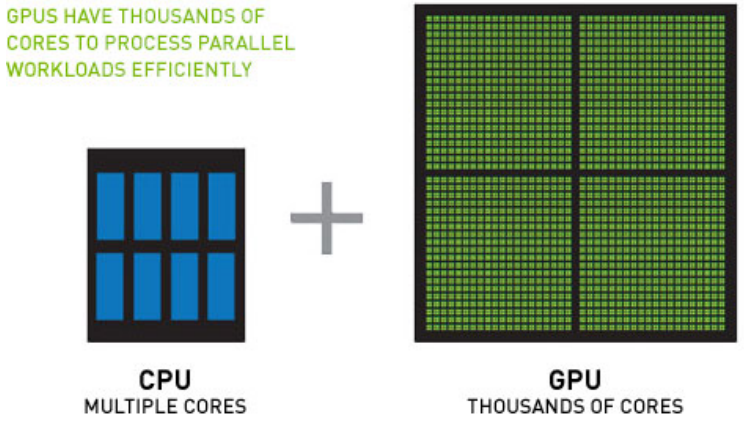
94^8= 6,095,689,385,410,816 possible passwords

Max. time: **55.000 years**

STRONGER

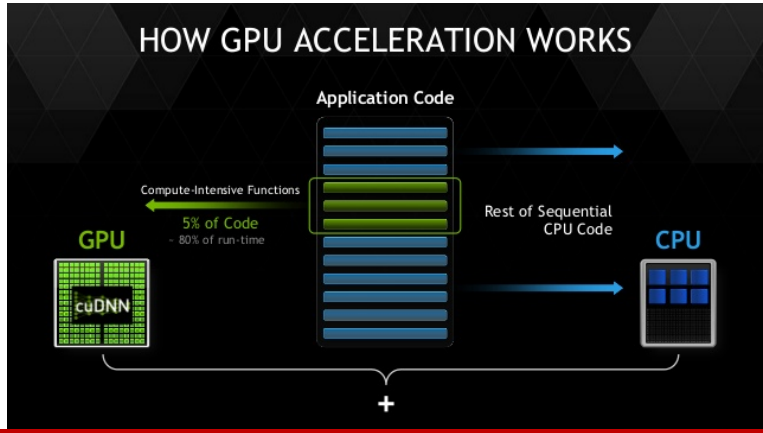
GPU Acceleration

- Gaming video cards output 60 fps of lifelike 3D rendering
- Video cards are used for mining crypto-currencies
- They are faster than the CPU
  - **Much faster**
  - **Getting faster every year**
  - **Intel i7: 15% performance increase between adjacent generations in 1 year**
  - **NVIDIA GeForce: 70% performance increase in 1 year (within the same family)**



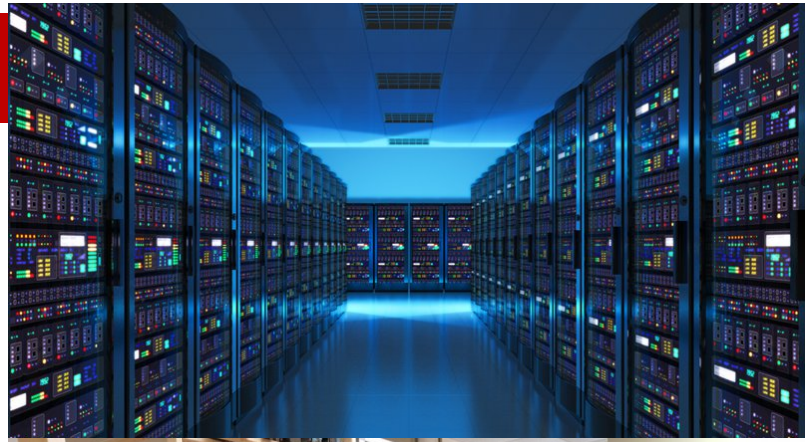
GPU Acceleration

- **Always use GPU units to speed up recovery**
- Real-world gain vs. a high-end quad-core i7:
  - 50x acceleration with a single video card
  - 200x acceleration with 4 video cards
  - Unlimited number of GPUs supported



GPU Farms

Advertisement >>>>>>>>>>>>>>>>>>



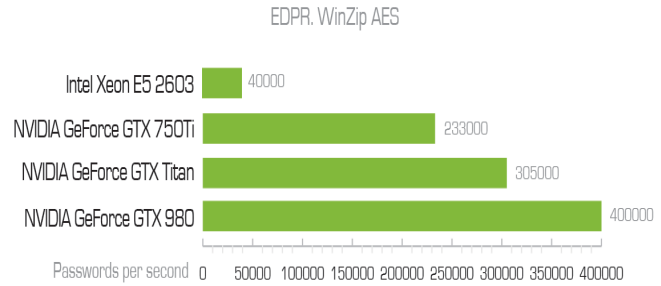
Real life >>>>>>>>>>>>>>>>>>>>>>>>

GPU Acceleration

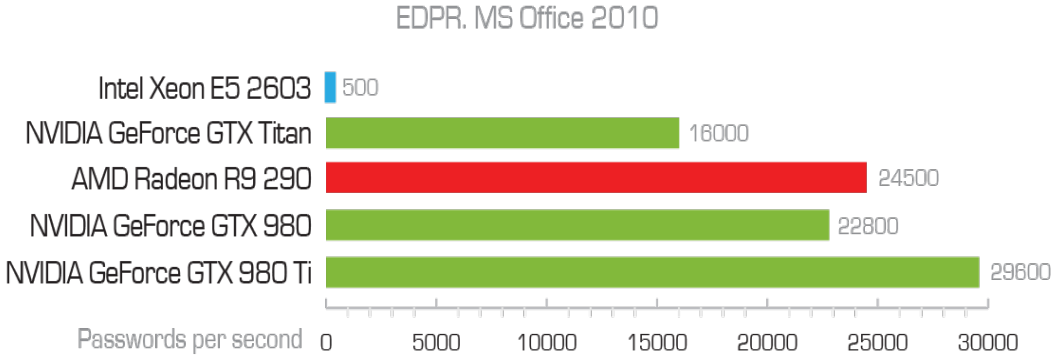
- **To do:**
  - Choose products with GPU acceleration
  - Install multiple GPUs
  - A single GPU reduces password recovery times 50 to 200 times
  - Lifehack: use multiple video cards of different makes, models and generations (including AMD and NVIDIA boards in a single PC)
- **Best practice:**
  - Invest in a GPU, not CPU
  - Buy additional cards, keep old ones, use them together for maximum benefit

GPU Acceleration

- **Real-world benchmarks**
  - Office 2010: 500 pwd/s (CPU) vs. 22800 (GPU)
  - WinZip AES: 40,000 vs. 400,000

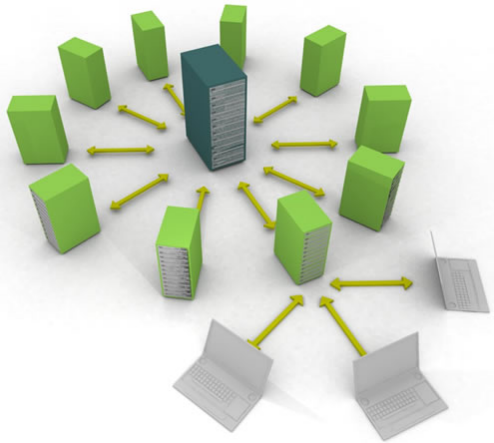


Intel Xeon E5 2603 vs.
NVIDIA GeForce GTX 980



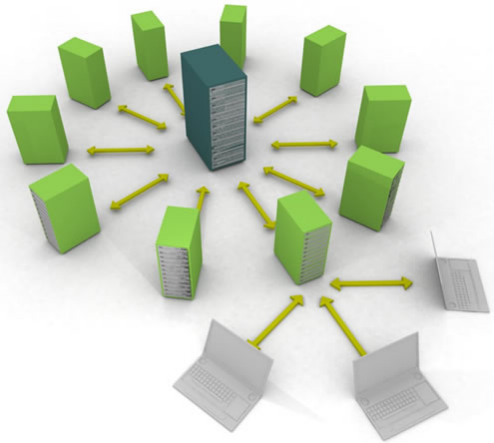
Distributed Computing

- **Sometimes, a single PC is not enough**
- Attack passwords over the network
- Multiple computers (each with GPU units) attack the same password in parallel
- Real-world benefit depends on scalability implementation



Distributed Computing

- **To do:**
  - Use distributed attacks
  - Zero scalability overhead: 10,000 computers will break the password 10,000 times faster than a single PC
- **Best practice:**
  - A single PC with a GPU is better than a network of 50 computers
  - A network of computers with GPUs achieve performance in teraflops range



MS Office 2013

Slightly stronger than average: 8 characters (upper and lower case letters, special characters and numbers combined)

94^8= 6,095,689,385,410,816 possible passwords

Max. time: **55.000 years : Raw power is not enough**

SMARTER

There is a catch!

About **60%** of passwords chosen by AVERAGE users

can be usually broken **within first two hours*!**

*) 10 instances, using GPU accelerator

There is a catch!

About **30%** of passwords choosen by AVERAGE users

can be usually broken ~~within first two hours~~*!

In minutes!!!

*) *10 instances, using GPU accelerator*

MS Office 2013

Average: 7 characters (upper and lower case letters and numbers)

62^7= 3,521,614,606,208 possible passwords

~~**277.292 hours (31.5 years)**~~ ~~**2 hours**~~ **In minutes**

How Is It Possible?

Main rule: most passwords are re-used

The 50 Most Used Passwords

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

Common Passwords

- **Top 25 passwords represent 2.2% of all passwords used**
- **Top 500 passwords represent 9.1% of all passwords used**
- A dictionary of 10,000 most common passwords helps solve up to 30% cases in almost no time
- 59% of consumers reuse passwords

Common Passwords

- **Best practice:**
  - Try breaking easier files first to obtain existing passwords
  - Use preliminary attacks to try common passwords
  - Use **Internet Password Breaker** to extract existing passwords

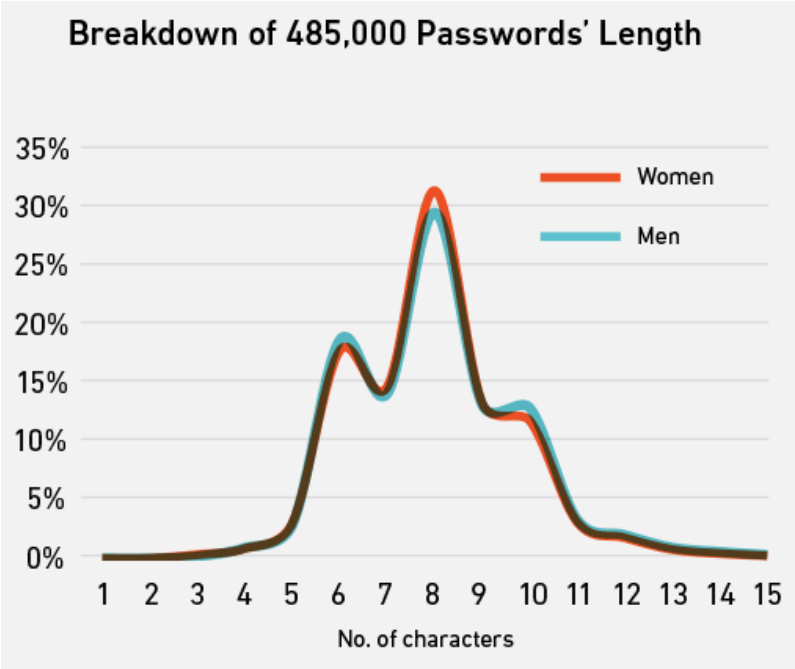
What Users think?

"I'll Add a Number to Make it More Secure."

Most Used Numbers (0-99) at the End of Passwords			Least Used Numbers (0-99) at the End of Passwords		
1.	examplepassword**1**	23.84%	100.	examplepassword**39**	0.15%
2.	examplepassword**2**	6.72%	99.	examplepassword**49**	0.16%
3.	examplepassword**3**	3.86%	98.	examplepassword**60**	0.17%
4.	examplepassword**12**	3.55%	97.	examplepassword**38**	0.18%
5.	examplepassword**7**	3.54%	96.	examplepassword**37**	0.18%
6.	examplepassword**5**	3.35%	95.	examplepassword**41**	0.18%
7.	examplepassword**4**	3.19%	94.	examplepassword**61**	0.18%
8.	examplepassword**6**	3.06%	93.	examplepassword**46**	0.19%
9.	examplepassword**9**	2.91%	92.	examplepassword**53**	0.19%
10.	examplepassword**8**	2.89%	91.	examplepassword**48**	0.19%

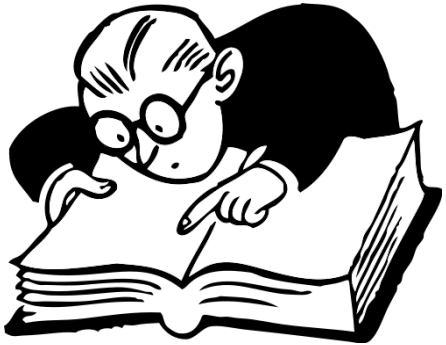
Evaluating Password Entropy

How many characters make a password secure?



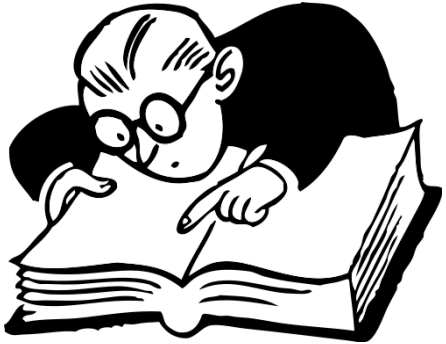
Smart Dictionary Attacks

- **Most consumers choose passwords based on dictionary words**
  - Sometimes appending a number
- **Security policies rarely block dictionary-based passwords**
  - Enforcing minimum length and use of numbers/special characters
- For strong protection (e.g. Office 2010-2016), dictionary is the only way to go
- In real world, dictionary attacks have ~50% success rate



Smart Dictionary Attacks

- **To do:**
  - Use pre-installed dictionaries
  - Dictionary attacks with pre-configured mutations come first
  - Followed by brute-force attack
- **Best practice:**
  - Build your own custom dictionary for each individual case
    We suggest **Proactive System Password Recovery**
  - Don’t waste too much time with standard dictionaries of common words.
    Using a smaller, targeted dictionary works much better
  - Use English and native words
  - Allow reasonable mutations
    Overshooting mutations may defeat the purpose



Common passwords

Most Used Base Phrase (4+ characters)	Most Used Noun (1,000 most common)	Most Used Verb (1,000 most common)	Most Used Colors (Used with numbers)
1. password	1. master	1. welcome	1. red
2. qwerty	2. football	2. enter	2. blue
3. qwer	3. killer	3. please	3. black
4. dragon	4. angel	4. flash	4. green
5. qazwsx	5. summer	5. chase	5. white
6. alex	6. money	6. catch	6. pink
7. love	7. freedom	7. express	7. orange
8. monkey	8. access	8. enjoy	8. brown
9. master	9. green	9. remember	9. purple
10. shadow	10. silver	10. rescue	10. yellow

Passwords from various sources leaked

2012
Court Ventures (200 mil), Massive American Business Hack (160 mil)

2014
eBay (145 mil), Target (70 mil), Home Depot (36 mil), Anthem (80 mil)

2015
JP Morgan Chase (76 mil)

Top 10.000.000 Real Passwords

IT security analyst
Utah, USA

What we analyzed? 10.000.000 passwords collected by Mark Burnett

https://archive.org/details/10MillionPasswords

All passwords are collected from 2011 to present days

A 98.8% recovery rate during the first minute?

Unfortunately, today a simple dictionary attack using the Top-10,000 passwords list brings modest results (about 30% success rate at best)

In order to achieve a higher success rate, we used our extensive knowledge and experience with desktop-based password recovery tools (we sold several hundred thousand of those during the past few years).

Mutations and dictionary attack. Best strategy.

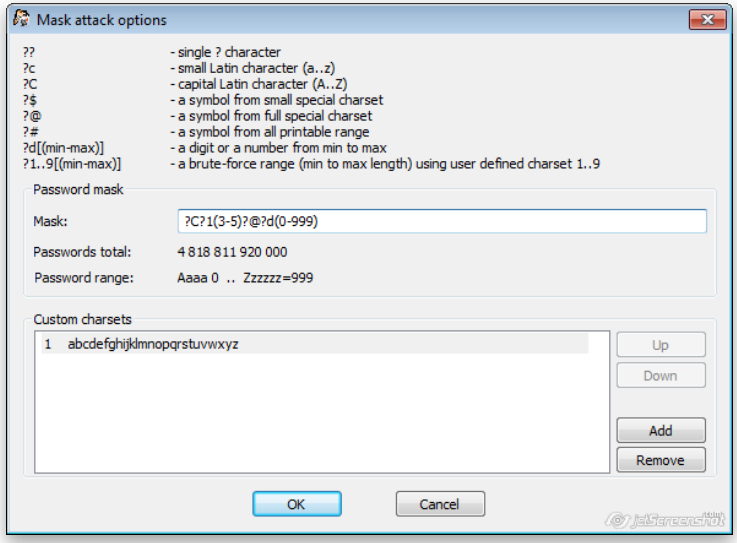
After extensive research and nearly half year of testing, we settled on the following attacks:

- **Top-100 passwords.** This dictionary attack uses the original Top-100 Passwords list including variations (appending up to 2 numbers and trying single-word and two-word combinations).

- **Top-10,000 passwords.** This attack with the dictionary containing top-10,000 passwords including simple variations (one number appended to the end of the password).

Advanced Attacks

- If there is a common pattern to user's passwords
- If there is a password security policy in place
    - **Advanced attacks can target that pattern**
- There are common mutation rules
- Dates and l33t language
- Mirror, rotate, duplicate, reverse, truncate, adjust character cases and more: ~40 customizable rules



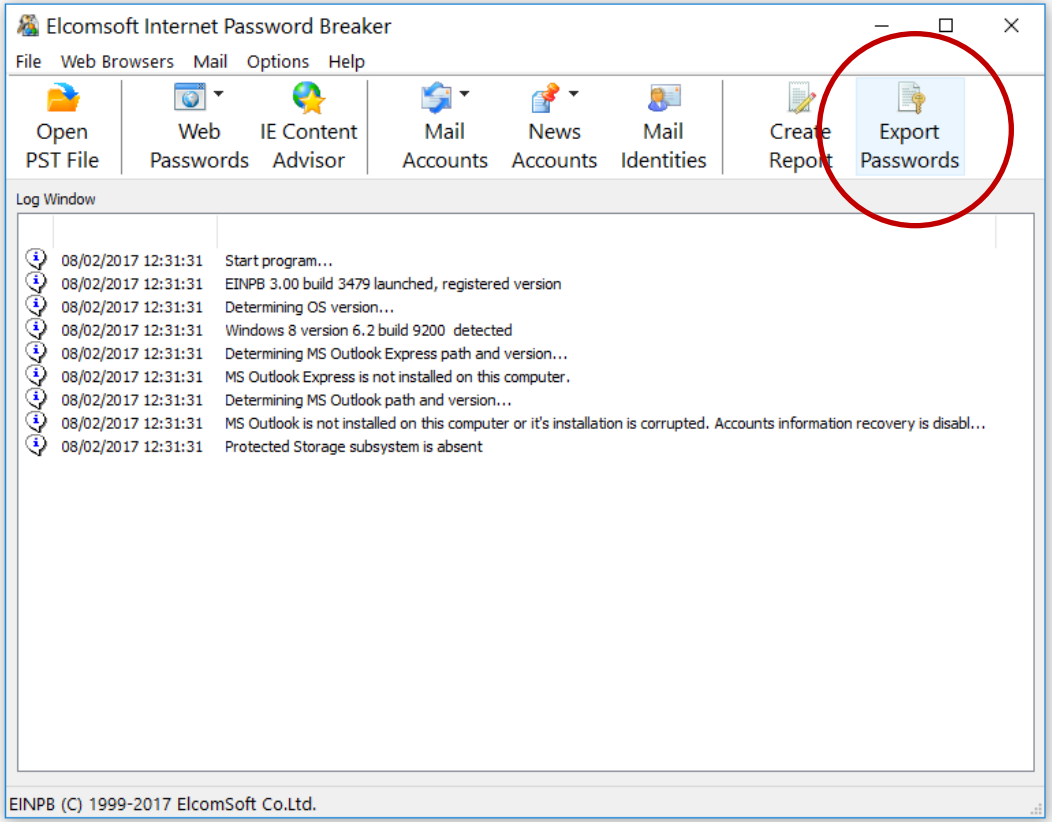
Strategy. Conclusion.

Step 1

- Acquire passwords that can be recovered instantly or in reasonable time at first
- Use **Elcomsoft Internet Password Breaker** to instantly extract passwords
- Try this passwords list on time-consuming documents (MS Office 2010-2013, for example)

Step 1

- Use **Elcomsoft Internet Password Breaker** to instantly extract passwords



Step 2

Analyze known user passwords and use simple mutations or mask method, if known passwords are build on some rules, of course

Example:

AlEx1234
aLeX4321
1Alex1
E1com$oft
eLCoMSoFT

Step 3

Use numbers-only brute-force. It will take split seconds

Step 4

Use Top-100/10.000 passwords dictionary without mutations (at first)

Step 5

Use language specific passwords dictionary without mutations

** We separated common passwords list into language specific dictionaries. For example – english, german, russian, etc.*

** Basic dictionaries are included in the program distribution. Additional dictionaries are available for purchase and immediate download.*

Step 6

Use brute-force with reasonable time settings (dictionary with mutations)

Step 7

Use brute-force ☹

QUESTIONS?

Breaking Passwords
Breaking Passwords and Overcoming Encryption

Vladimir Katalov, ElcomSoft Co. Ltd.

Facebook: ElcomSoft
Twitter: @elcomsoft