Password Hardening using ML based algorithms

Nividh Singh

Cybersecurity

- Cybersecurity is the practice of deploying people, policies, processes and technologies to protect organizations, their critical systems and sensitive information from digital attacks
- The goal of cybersecurity is to prevent malicous users from gaining access to systems or information

Cybersecurity – Data Transfer

- Two main algorithms: AES and RSA
- RSA
  - Use public and private keys
  - Really secure because they use large prime numbers
  - Hard to get private keys because there’s no algorithms or large enough computing power to factor the numbers
- AES
  - Symetric Keys
  - Block Encrpytion

Social Engineering

- Social engineering is the term used for a broad range of malicious activities accomplished through human interactions.

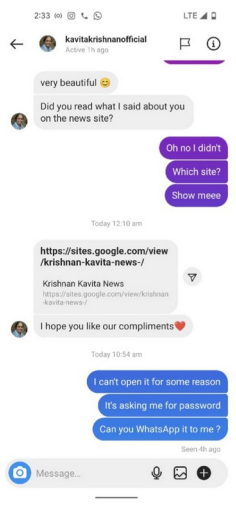

Image 1: Hacker impersonating Kavitha Krishanan sends out a malicious Google Sites link

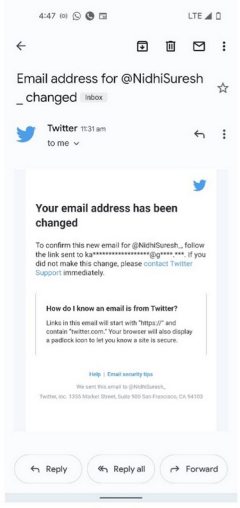

Image 2: Email from Twitter saying account email has been changed.

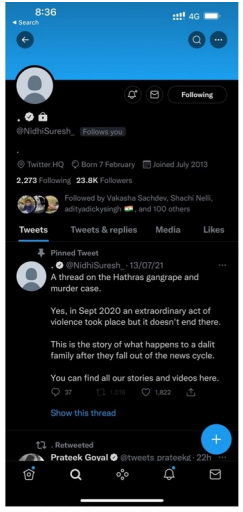

Image 3: The hacker takes control of Nidhi Suresh's Twitter account and changes name, image, background.

Password Hacking

- In cryptanalysis and computer security, password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system in scrambled form.
  - Some how hack into the system and find the password
  - Use brute force to “guess“ the password

Password Hacking

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

HIVE SYSTEMS

› Learn about our methodology at hivesystems.io/password

Password Hacking

Samples

54429863asd
mschadock123
Anjani3737
vadabepu
QYIN
5139210maddog
cjohn1992
redlines2754
15275therese
24780844
0505907243
d3toxifi3d
mgsltd
1784mamaq
669Punk
gozabetu
cp57ji4bwnavy2
asta4882
eb3-R1#a7n
shkilnyy
uciteljica123

654123ff
aryxu1981
y6nkg
0o6kc9
batugosh
21545876112578
50bdd1
BLUEABA2
78Apollo
gamscakht7ty9vc5
shvec-tany
220576000
3991seivadwb1123
8012f5ef
lorinoack
84254772
1e3e416ac6f9d7bd2c
belukone
izSGMvcF8W9Ti38Mg
73ani35hch
nsonazo

Orangeceltics
jinnam1234
murdocfan1
8oqep
773193283
andragatli
funseeker4347
THO1MAS777
snooch151
sumria201
fb863210392
anjers305
73Ekmrfcfh73вЂ
01628786291
bandisreenivasulu
EwSC
0935644115q123
6446445vikap
odinschild
198403061215
AlejHD

gr1686
emmaprofileimage
padela13
peanutclock
nurjei0608
dyduloty
TaaCVc
themorpheus91
danran2319
Zouz123654
36D817
ilovesuzy0429
rabha200880
390683aa
asd0983229827
2b73004faf006983774651a803a2ab33
davidevendetta123
i04s6
khongkimthanh
3738113234
6978556589

voqyvome
mne18fbs
Tani823
sezgin6565
svietlana.sidorkina
hanomari
baka^_^
aleksey0504
pomple8155
5891milsum
991570
ossi6620
EJNIH
adrianazarel9602211

Ethical Hacking

- Hacking to prevent the effect of malicious attacks
- Prepare systems to be robust against attacks

Algorithms

Alphabetical Order

- Tests the passwords in alphabetical order
- Algoirthms can have different “alphabetical orders“
  - Some might put numbers before letters
  - Some might put uppercase seperate from lowercase

Good Passwords	Bad Passwords
2b73004faf006983774651a803a2ab33	andragatli
73ani35hch	eb3-R1#a7n
svietlana.sidorkina	Anjani3737

Probabilistic Order

- Takes in all the passwords that have been linked
- Breaks the passwords down into subsets of charectors
- Uses machine learning to try to predict the next charector from the previous charectors

1 → 2 → 3 → 4 → 5 12345

1 → 2 → 3 → 4 → 6 12346

English Words

- This algorithm takes a library of english words and puts charectors between them
- (charectors(s)) + word + (charectors(s)) + word + (charectors(s)) = password
- eg. 78 + Apollo = 78Apollo

Good Passwords	Bad Passwords
2b73004faf006983774651a803a2ab33	emmaprofileimage
21545876112578	ilovesuzy0429
gamscakht7ty9vc5	78Apollo

Results & Conclusion

- The more methods that were used, the more passwords were labeled as not secure
- There were a lot of passwords in the databases that weren’t good passwords
- Using this type of model would work better instead of the 12 charector, 1 number, 1 special charector, 1 uppercase and 1 lowercase letter approach

Future Steps

- Implement more methods for hacking, so more weak passwords can be taken out
  - Only use numbers (nnnnnn)
  - Only use letters (llllll)
  - Keep numbers grouped and letters grouped (nnnlll)
- Implement a custom training loop for better performance

Questions?