Chris Bugg
Chris Hamm
Jon Wright
Nick Baum

Password Security

- Password security is important.
- Users
  - Weak and/or reused passwords
- Developers and Admins
  - Choose insecure storage algorithms.
- Mighty Cracker
  - Show real world impact of poor password security.

OVERVIEW

- We made a hash cracker.
- Passwords are stored as hashes to protect them from intruders.
- Our program uses several methods to ‘crack’ those hashes.
- Networking
  - Spread work to multiple machines.
- Cross Platform

OTHER HASH CRACKING PRODUCTS

- Hashcat
- Cain and Abel
- John the Ripper
- THC-Hydra
- Ophcrack

- Network support is rare.

WHAT IS HASHING

- A way to encode a password to help protect it.
- A mathematical one-way function.

- MD5 hash
  - cf4ff726403b8a992fd43e09dd7b5717
- SHA-256 hash
  - 951e689364c979cc3aa17e6b0022ce6e4d0e3200d1c22dd68492c172241e0623

SUPPORTED HASHING ALGORITHMS

- Current Algorithms
  - MD5
  - SHA-1
  - SHA-224
  - SHA-256
  - SHA-384
  - SHA-512

WAYS TO CRACK

- Cracking Modes
  - Single User
  - Network Mode
- Methods of Cracking:
  - Brute Force
  - Dictionary
  - Rainbow Table
  - GUI or Console

BRUTE FORCE

- Systematically checking all possible keys until the correct one is found.
- Worst case this would transverse the entire search space.
- Slowest but will always find the solution if given enough time.

DICTIONARY ATTACK

- List of common passwords from leaks/hacks.
- Many people choose common passwords

- Written works of Shakespeare ~66,000 words
- Oxford English Dictionary ~290,000 words

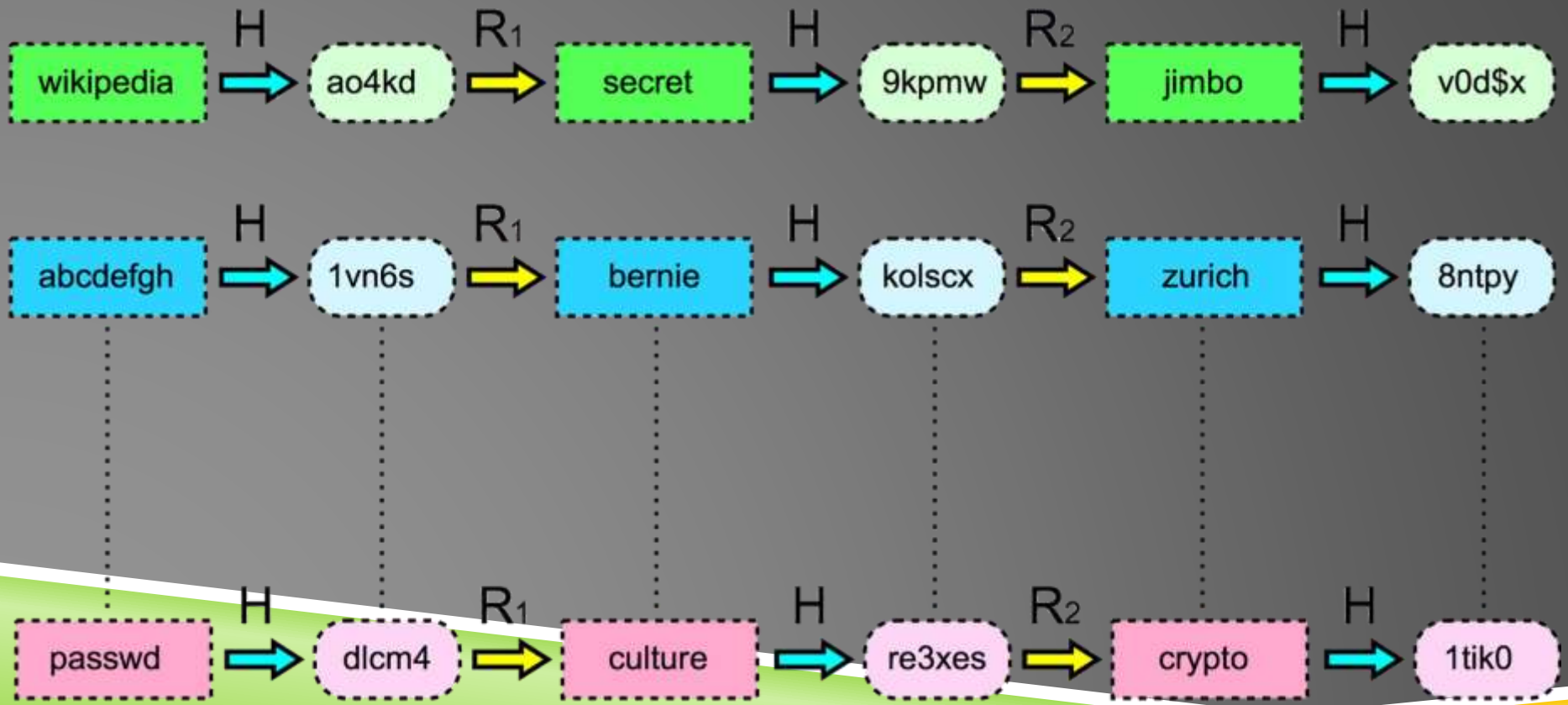
- Small dictionary = 900,000 words
- Medium dictionary = 14 million words
- Large dictionary = 1.2 billion words

RAINBOW TABLE

- Can’t store all possible hash/key combinations.
  - 16 character key = 10^40th combinations
  - 10^50th atoms on earth
- Rainbow tables
  - Reduced storage.
  - More computation.
  - Storage can still be immense.
- Far faster than other methods.

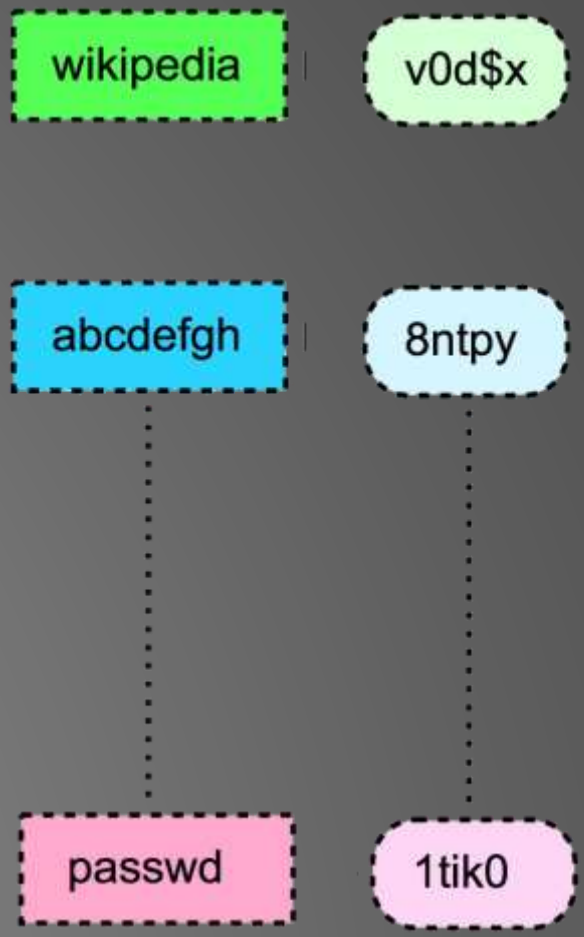
RAINBOW TABLE (HOW IT WORKS)

Tables are generated by repeated use of hash and reduce functions.



RAINBOW TABLE (HOW IT WORKS)

- Store only the initial key and final hash of each row.
- Middle part is easily reproducible.
- Storage requirements divided by the width of the table.



GUI DEMO


Mighty Cracker
File View Run
Mighty
Cracker
Single Mode
Network Mode
About Us
Close

GUI DEMO

*^n1gh7^m4r3^*[*123*]

- Stolen in 2009 data breach
- Don’t reuse passwords.

Time Required to Exhaustively Search this Password's Space:	
Online Attack Scenario: (Assuming one thousand guesses per second)	1.33 hundred trillion trillion centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	1.33 million trillion centuries
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	1.33 thousand trillion centuries

DEVELOPMENT

- Requires Python 2.7.X
- GUI Requires wxPython
- Pycharm
- Linux, OSX 10.6+, Windows 7+
- Git

WHY USE PYTHON?

- ♥ People love Python ♥
- Easy to learn the basics and get going.
- Something new compared to what we have learned.
  - C/C++, Java, C#, Haskell, OCaml, MySQL, Perl

CHALLENGES

- Global Interpreter Lock (GIL) in Python
  - Threads Run Serially, Not in Parallel
  - Caused many issues for networking
  - Solution was Python's multiprocessing library
- Pickling
  - wxPython objects are not pickleable

CHALLENGES CONTINUED

- Windows support
  - manager conflicts
  - fork vs. spawn processes
    - pickling issues
- Graphics Library
  - Tkinter - can’t handle complicated layouts
  - Solution was wxPython library
- Everyone knows “a little” python
  - In-depth help was hard to find

FUTURE PLANS

- Crash recovery
- “Pause” ability
- GPU Support
- Real-time Client Monitoring System for Server
- Re-Implement in C++
- More algorithms
  - LM (Windows ME and before)
  - NTLM (Windows XP → 8.1)

DEFEATING THE MIGHTY CRACKER

- Strong storage algorithms
  - bcrypt, scrypt
- Use long (12+ character) random passwords

  Don’t reuse passwords

  Two factor authentication
- Password manager
  - KeyFree, LastPass

Thank You

- Ruben Gamboa
- Jim Ward
- StackOverflow
- The Internet

QUESTIONS?

References

- GRC's Password Haystack - https://www.grc.com/haystack.htm
- "Rainbow table1" by Dake - Dake. Licensed under CC BY-SA 2.5 via Wikimedia Commons - https://commons.wikimedia.org/wiki/File:Rainbow_table1.svg#/media/File:Rainbow_table1.svg
- http://media.idownloadblog.com/wp-content/uploads/2013/06/OS-X-Mavericks-logo-full-size.jpg
- http://th03.deviantart.net/fs70/PRE/f/2012/312/7/3/microsoft___windows_8_logo_by_n_studios_2-d5keldy.png
- https://thinkboxly.files.wordpress.com/2012/04/linux_logo.png
- http://astroleaks.lamost.org/wp-content/uploads/2012/03/Logo_Python.png
- http://blog.jetbrains.com/wp-content/uploads/2014/02/pycharm_logo_square.jpg