Matt Christensen (mrc621)

November 1, 2021

CS 465 (001) – Clift, Frederic M

Project #7 – Password Cracking Report

**Experiment**

**Questions**

1. *Assuming that you used your setup for this lab alone, how long do you calculate that it would take to crack a 6-character alphanumeric password? 8-characters? 10-characters? 12-characters? (use the c/s measurement from your experiments).*
2. *Do you think that the password meter is a good indication of actual password security? From the results of your experiment, what is your recommendation for minimum password length? Be creative in your response. Imagine what hardware and resources a potential attacker might have, and briefly justify your assessment of the attacker’s capabilities.*
3. *Recently, high-end GPUs have revolutionized password cracking. One tool, [ighashgpu](https://www.darknet.org.uk/2016/08/ighashgpu-gpu-based-hash-cracking-sha1-md5-md4/), is able to perform 1.3 billion MD5 hashes per second on an AMD Radeon 5850 (a 2-year-old, mid-to-high range video card). [Whitepixel](http://whitepixel.zorinaq.com/), another tool, claims that it can perform 33.1 billion hashes per second using 4 Radeon 5970s. Consider your calculations in question #1, and redo them assuming you had access to a system with 4 Radeon 5970s. Do your answers for question #2 change?*
4. *Fedora 14 and other modern Linux distributions use a SHA-512 (rather than MD5) for hashing passwords. Does the use of this hashing algorithm improve password security in some way? Why or why not?*
5. *Does the use of a salt increase password security? Why or why not?*
6. *Against any competent system, an online attack of this nature would not be possible due to network lag, timeouts, and throttling by the system administrator. Does this knowledge lessen the importance of offline password attack protection?*
7. *OPTIONAL QUESTION: The sheer power of GPUs make John the Ripper pale in comparison, despite all the heuristics John the Ripper employs. With hardware continually becoming more powerful, do you foresee a day in the near future when minimal password lengths will be too large for a typical person to remember? If so, what types of vulnerabilities may arise from such a scenario? What would you recommend as the next step in password evolution?﻿*
8. *Extra Credit (5 points) Download and use hashcat. Compare usage to john the ripper.*
9. *Extra Credit2 (5 points) If you have your own hardware available, try to use hashcat with a GPU and compare CPU versus GPU hashing speeds for similar inputs.*