EÖTVÖS LORÁND TUDOMÁNYEGYETEM

INFORMATIKAI KAR

SZAKDOLGOZAT TÉMABEJELENTŐ

Hallgató adatai:

Név: Nagy Richárd Antal

Neptun kód: V7BFDU

Képzési adatok:

Szak: programtervező informatikus, alapképzés (BA/BSc)

Tagozat: Nappali

Belső témavezetővel rendelkezem

Témavezető neve: *Eichhardt Iván*

munkahelyének neve, tanszéke: Eötvös Loránt Tudományegyetem, Informatikai Kar, Algoritmusok és Aalkalmazásaik Tanszék

munkahelyének címe: 1117 Budapest, Pázmány Péter sétány 1/C.

beosztás és iskolai végzettsége: oktató, PhD

A szakdolgozat címe: Titkosított Jelszavak Feltörésének Gyorsítása GPU Parallelizációval

A szakdolgozat témája:

(A témavezetővel konzultálva adja meg 1/2 - 1 oldal terjedelemben szakdolgozat témájának leírását)

Napjainkban szinte minden program és platform amit használunk egy távoli szerverrel kommunikál, amelyhez a rendszereknek egy nem biztonságos csatornán keresztül kell beazonosítania a felhasználót. Általánosan valamilyen azonosító és jelszó megadásával.
A megadott jelszót a szervernek valamely formában tárolnia kell, hogy sikeresen el tudja végezni a felhasználó azonosítását. Ezek tárolására egy általános és a kisebb rendszerekben is használt megoldás a jelszó [1] hash-algoritmussal való egy-irányú titkosítása.
Ezeket a hash-eket "visszafelé" nem lehet lefuttatni, ezért kizárólag próbálkozással törhető fel. Ezen próbálkozás azonban egy parallelizálható folyamat videókártya segítségével, ugyanis az egyik hash elkészítése nem befolyásolja a többit. A hash folyamat egyik fontos lépése a sózás (salt) ami még egy komplexitási réteget ad a feltörésükhöz.
A feltöréshez fontos részt fog képzeni egy olyan [2] jelszó táblázat használata, amely a gyakran használt jelszavakat tartalmazza, ezáltal jelentősen leszűkítve a lehetséges próbálkozások számát.
A szakdolgozat célja a releváns technikák bemutatása és egy olyan program elkészítése, amely egy megkapott hash kódot megpróbál feltörni videókártya segítségével, illetve ezen projekt optimalizálása a lehető legmagasabb sebesség elérése érdekében. A projekhez az [3] ELTE IK GPGPU tantárgy anyagát fogom alapul venni.

[1] Hatzivasilis, George. "Password-hashing status." Cryptography 1.2 (2017): 10.
[2] https://haveibeenpwned.com/Passwords Jelszó Lista (2020.11.25)
[3] ELTE IK Algoritmusok és Alkalmazásaik Tanszék, Computer Graphics GPGPU tantárgy anyaga: http://cg.elte.hu/index.php/gpgpu/ (2020.09.14)

Budapest, 2021.01.22.