Economics of Password Cracking in the GPU Era

8/3/2011

Robert Imhoff-Dousharm

Achieve More.

Overview

- Introduction
- GPU Cracking
- Economics
- Deployment Explained
- Lessons Learned
- Conclusion
- Q/A

Shameless Plugs…

- Atheros Communications
  - Initial research time and funds
- SanDisk Corporation
  - Continued time and funds
- People of earth
  - "Acting Human"
- Electricity
  - Provides the "path of least resistance"
- Vegas 2.0 – dc949 – CuckooNest

About me…

- Research and technical – IT Security
  - 4 years Credit card security (see DEF CON 11-13)
  - 3 years code IDPS research
  - 2 years GPGPU password cracking
- Suit and Tie
  - 12 years working experience with IT Security
  - Developer – Researcher – SOC Analyst – Response – Tactical – Holistic
- Private Hack Space
  - We have tree's and servers to muse over

Overview: Introduction

Introduction

- What is General Computing?
  - GPU vs SSE*x* vs. HPC
    - CUDA and OpenCL (not GL)
  - What is the current state of GC and HPC?
    - Top500
- Cloud Computing
  - Amazon AWC / EC2
  - Nimbix
  - Peer1 Hosting
  - Penguin Computing

Introduction

- Distributed Technologies
  - distributed.net
  - Folding@home
  - SETI@home
  - BitCoin

Overview: GPU Cracking

GPU Cracking – Hardware

- NVidia vs. ATI
  - GTX 590
    - 1024 Cores * 8 Cell = 8,192 “streams”
  - Radeon HD5870
    - 1,600 “Cores” == 1,600 Streams
- CUDA vs. Stream vs. OpenCL
  - CUDA == R.A.D
  - Stream == Piss poor documents
  - OpenCL == Wave of future (sorry CUDA)

GPU Cracking – Software

- Current offerings
  - oclHashCat
  - igHash
  - CUDA-Multiforcer (M.I.A)
- Current Benchmarks
  - NTLM (Windows AD)
  - MD5 (Websites)
  - Salt based passwords (Smart)

GPU Cracking – Software

- What's in a mask?
  - Character Minimum
  - Upper, lower, special and numeric
  - Passphrase concepts
- Two factor and you!
  - Google Authenticator
  - Symantec VIP
  - SecureAuth
  - RSA SecurID (giggle)

Overview: Economics

Economics

- Locally hosted
  - Single box
  - Private Cloud
  - Local Distribution (custom Screen Savers, etc.)
- Public Cloud
  - Amazon / Peer1 / Penguin Computing
  - LastBit / ElcomSoft (!= good)
- Distributed
  - Non existing?

GPU Password Cracking Video Card Matrix

GPU	GTX295	M2050	GTX470	GTX480	GTX570	GTX580	HD5870	GTX590*
Cores	240	448	448	480	480	512	1600	1024
Memory	896	3072	1280	1536	1280	1536	1024	3072

	Keys Per Second (In Millions)							
CMF Alpha 0.8r4	693.80	1152.18	1323.75	1722.58	1798.77	2020.43	n/a	4200.00
HashCat 0.24	732.70	n/a	819.78	1290.70	1347.80	1357.50	2906.00	2700.00

	Password Length: 8							
Hours	2510.27	1511.59	1315.68	1011.06	968.23	862.01	599.32	414.67
Days	104.59	62.98	54.82	42.13	40.34	35.92	24.97	17.28
Years	0.29	0.17	0.15	0.12	0.11	0.10	0.07	0.05
Centuries	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Galactic Years	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

GPU's	Days to Complete								
2	52.30	31.49	27.41	21.06	20.17	17.96	12.49	8.64	†
4	26.15	15.75	13.70	10.53	10.09	8.98	6.24	4.32	‡
16	6.54	3.94	3.43	2.63	2.52	2.24	1.56	1.08	◊
20	5.23	3.15	2.74	2.11	2.02	1.80	1.25	0.86	
32	3.27	1.97	1.71	1.32	1.26	1.12	0.78	0.54	
100	1.05	0.63	0.55	0.42	0.40	0.36	0.25	0.17	
250	0.42	0.25	0.22	0.17	0.16	0.14	0.10	0.07	
500	0.21	0.13	0.11	0.08	0.08	0.07	0.05	0.03	
1000	0.10	0.06	0.05	0.04	0.04	0.04	0.02	0.02	
10000	0.01	0.01	0.01	0.00	0.00	0.00	0.00	0.00	
100000	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	

List Price	$290.00	$2,500.00	$260.00	$425.00	$325.00	$490.00	$320.00	$740.00
Keys / Dollar	2.39	0.46	5.09	4.05	5.53	4.12	9.08	5.68
Keys / Core	2.89	2.57	2.95	3.59	3.75	3.95	1.82	4.10
Key / Memory	0.77	0.38	1.03	1.12	1.41	1.32	2.84	1.37

*Estimated speeds

†2x ATX Setup

‡4x eATX Setup

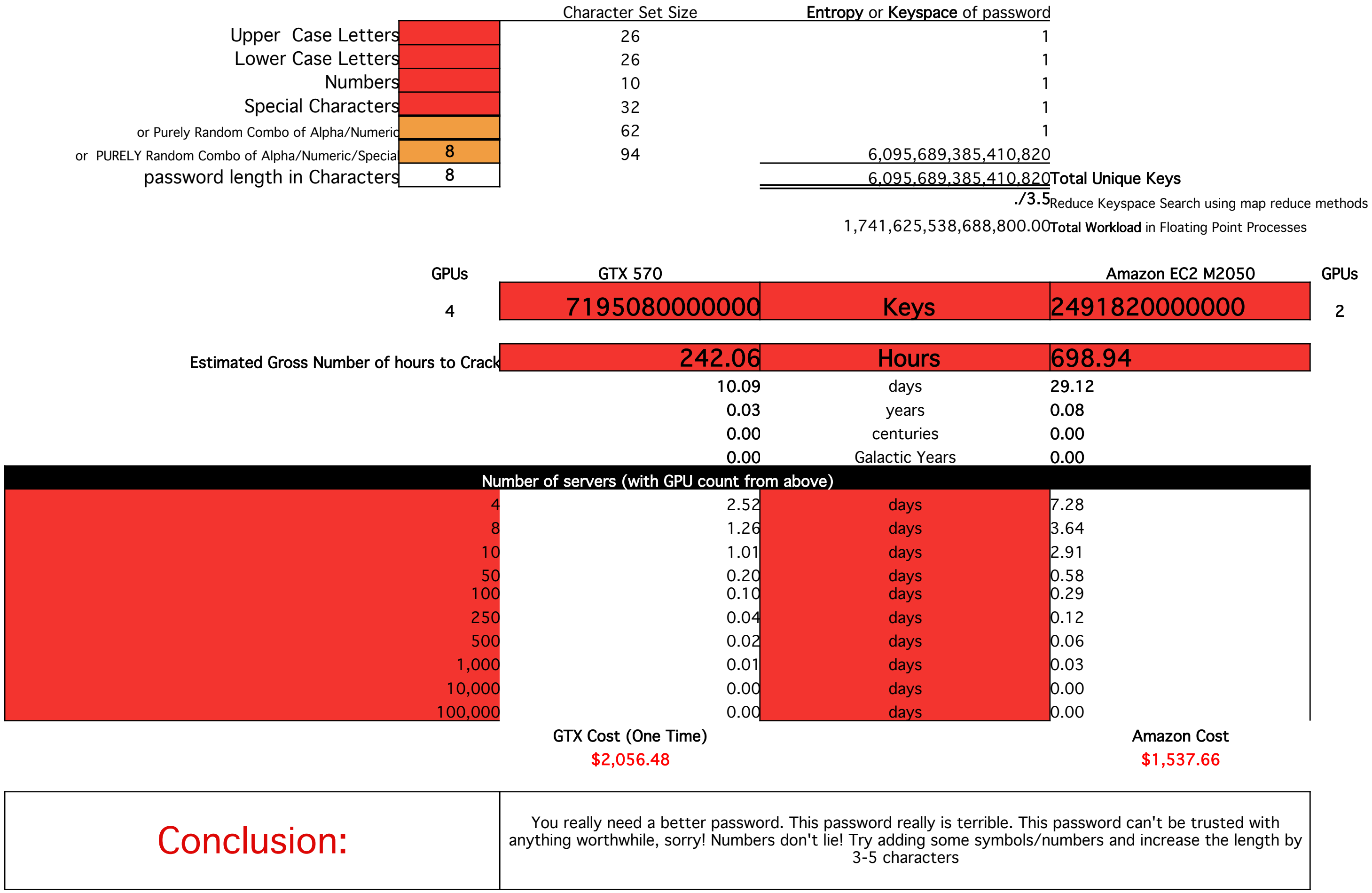
◊16x Chassis (Dell C410x / Cubix Expander)

Example "Super Computer" GPGPU Setup

SKU	Description	QT	Unit Cost	Total Cost
Super B8DTG	Supermicro SBI-7126TG Intel 5520 LGA1366 GPU Blade	10	$699.84	$6,998.40
AOC-IBH-XQS	Supermicro Add-on Card AOC-IBH-XQS Network adapter	10	$550.70	$5,507.00
BX80602E5506	Intel Xeon E5506 Nehalem-EP 2.13GHz 80W Quad-Core Server Processor	20	$230.00	$4,600.00
GTX590	GeForce GTX 590 (Fermi) 3072MB 768-bit GDDR5 PCI Express 2.0 x16	20	$749.99	$14,999.80
MCP-640-00062-0N	Accessory MCP-240-00062-0N FH L-Bracket for Standard-LP 4XLANCARD Retail	20	$20.70	$414.00
N8G-ST2	Active Media Products Amp 8GB 7-Pin SATA Dom Flash Disk	10	$75.90	$759.00
KVR1333D3D4R9S/8G	Kingston 8GB 240-Pin DDR3 SDRAM ECC Registered DDR3 1333 Server	20	$175.00	$3,500.00
Super SBE-720E-R75	Supermicro SuperBlade SBE-720E-R75 Rack-mountable	1	$3,587.63	$3,587.63
SBM-IBS-Q3616	Supermicro Blades SBM-IBS-Q3616 - SB Infiniband Swch 40gb INFINISCALE	1	$5,318.77	$5,318.77
SBM-XEM-X10SM	Supermicro - SBM-XEM-X10SM - SBLADE L3 10gbe Swch 480gbps Layer3 10g	1	$7,153.27	$7,153.27
			Total	**$52,837.87**

GPU Count	Pass/GPU	Total /Sec
40	3.42	136.8

Password Brute Force Calculator



		Character Set Size	Entropy or Keyspace of password	
Upper Case Letters		26	1	
Lower Case Letters		26	1	
Numbers		10	1	
Special Characters		32	1	
or Purely Random Combo of Alpha/Numeric		62	1	
or PURELY Random Combo of Alpha/Numeric/Special	8	94	6,095,689,385,410,820	
password length in Characters	8		6,095,689,385,410,820	Total Unique Keys
			./3.5	Reduce Keyspace Search using map reduce methods
			1,741,625,538,688,800.00	**Total Workload** in Floating Point Processes

GPUs	GTX 570		Amazon EC2 M2050	GPUs
4	7195080000000	Keys	2491820000000	2
Estimated Gross Number of hours to Crack	242.06	Hours	698.94	
	10.09	days	29.12	
	0.03	years	0.08	
	0.00	centuries	0.00	
	0.00	Galactic Years	0.00	

Number of servers (with GPU count from above)			
4	2.52	days	7.28
8	1.26	days	3.64
10	1.01	days	2.91
50	0.20	days	0.58
100	0.10	days	0.29
250	0.04	days	0.12
500	0.02	days	0.06
1,000	0.01	days	0.03
10,000	0.00	days	0.00
100,000	0.00	days	0.00
	GTX Cost (One Time)		Amazon Cost
	$2,056.48		$1,537.66

Conclusion:	You really need a better password. This password really is terrible. This password can't be trusted with anything worthwhile, sorry! Numbers don't lie! Try adding some symbols/numbers and increase the length by 3-5 characters

Overview: Deployment Explained

Deployment Explained

- Live Amazon EC2 Demo
- Live oclHashCat Demo
- Live CUDA-Multiforcer Demo

Overview: Lessons Learned

Lessons Learned

- NTLM and your environment
- Gawker, Sony and others *or*
  - “How I got F’ed in the A with a D…prison style”
- The 8-Char password
- Salting passwords and the future
  - Really this is NOT as superficial as you would think!
- ♪ In the year 2000! ♪
  - Near Future Cracking Number
  - Next 1-2 Years Cracking Numbers
  - Quantum Computing

Overview: Conclusion

Q/A

Robert Imhoff-Dousharm

the Hackajar

@hackajar

Facebook.com/hackajar

Linkedin.com/hackajar