Advanced BT5:personal HPC

...and implications for security architecture

HASK
May-29-2012

Overview

- Context
- Backtrack5
- CPU Intensive apps
- Back Track: HPC, Old School
- Spin Forward: MNC and other meaningful pastimes
- Poor man (smart man) HPC
- Putting the bits together

Context

Tim Chipman
Fortech I.T. Solutions
http://FortechITSolutions.ca

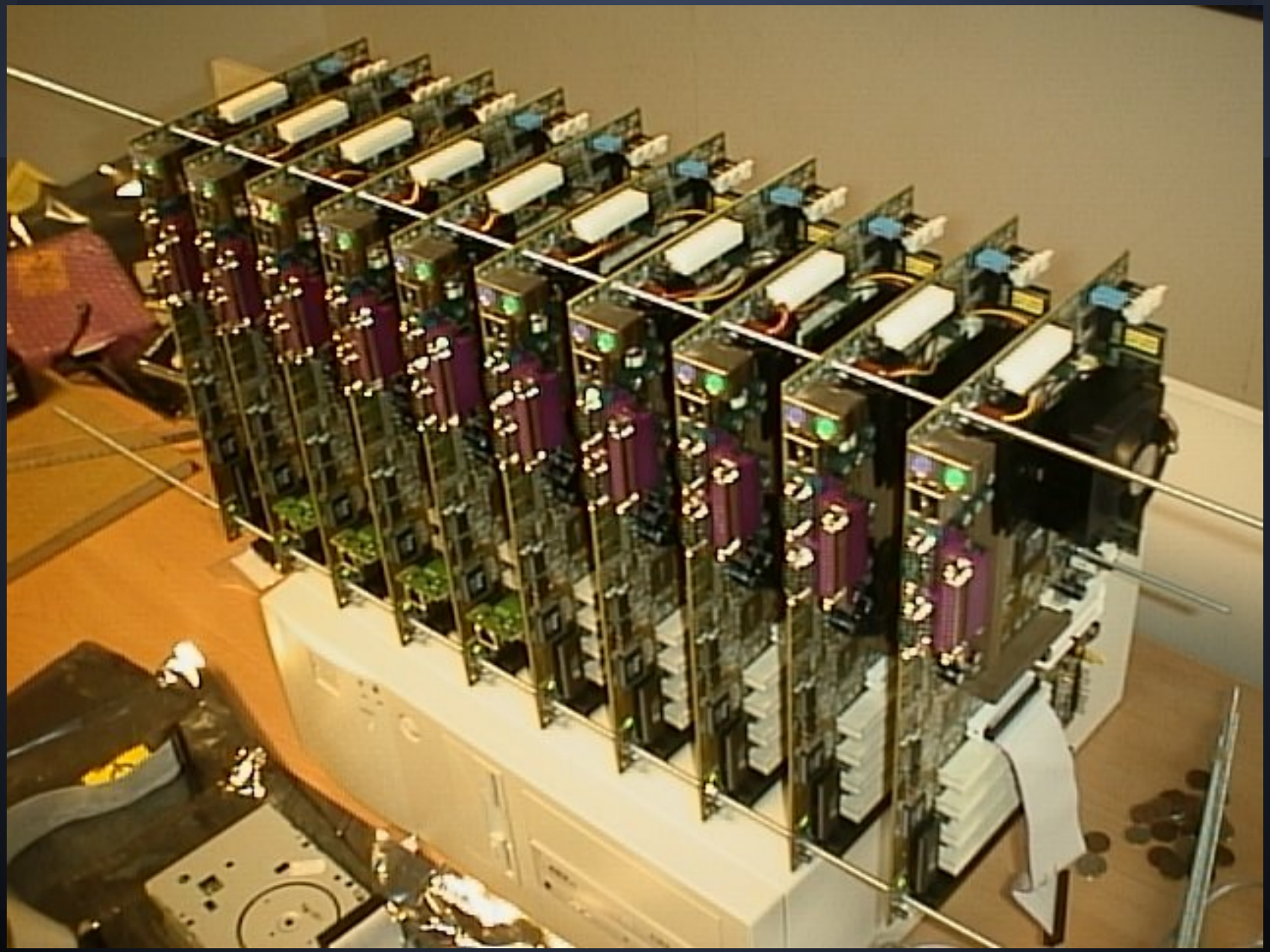
"HPC is Fun"

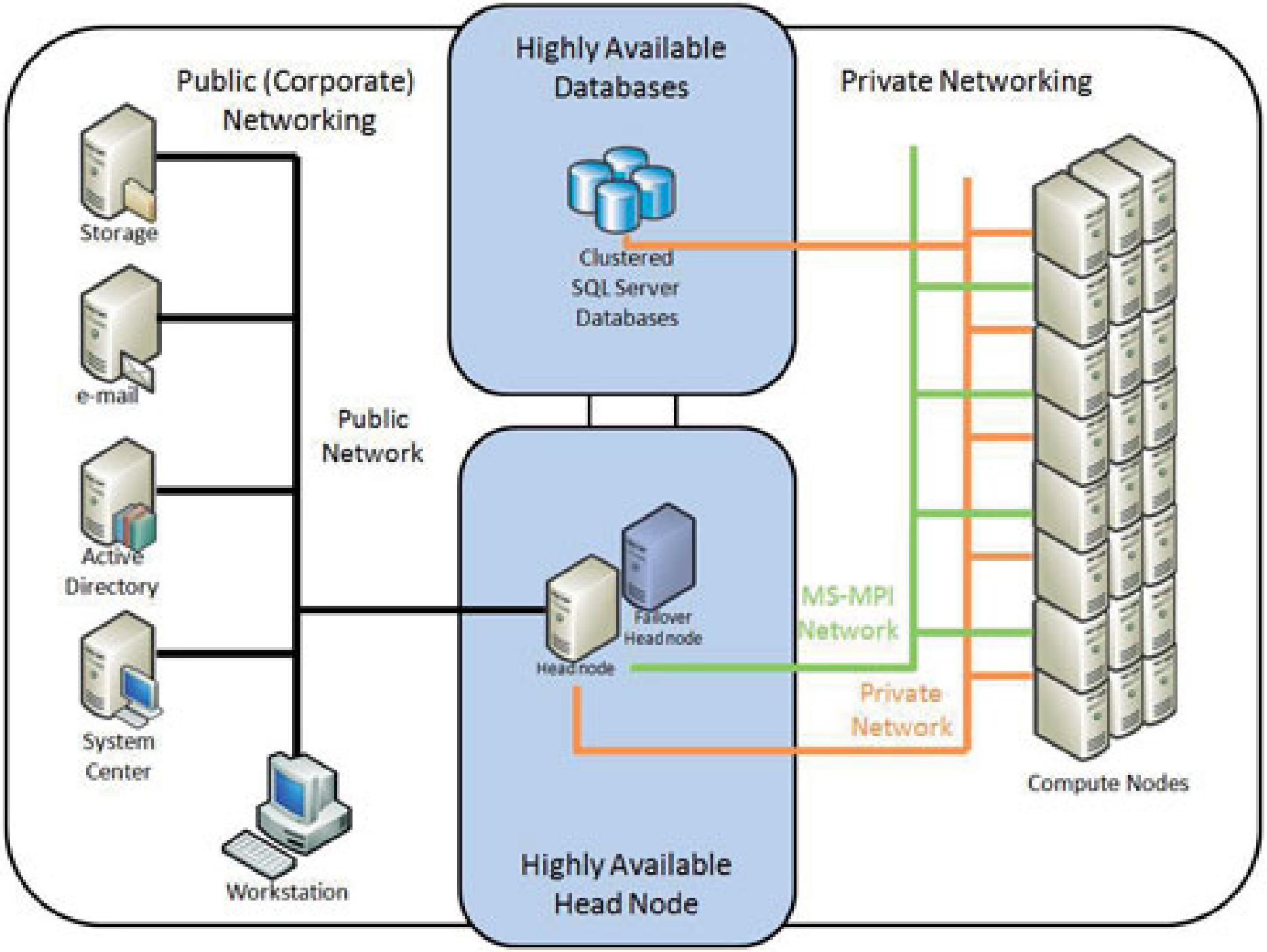
BackTrack5

- Well established tool set for pen testing, security audits
- Brute force tools - CPU intensive
  - brute force password cracking (NTLM, shadow, etc)
  - WPA - generation:test:crack
  - encrypted archives (RAR)
- It turns out there is an easier (and cheaper) way than buying a quad+socket server for $50k

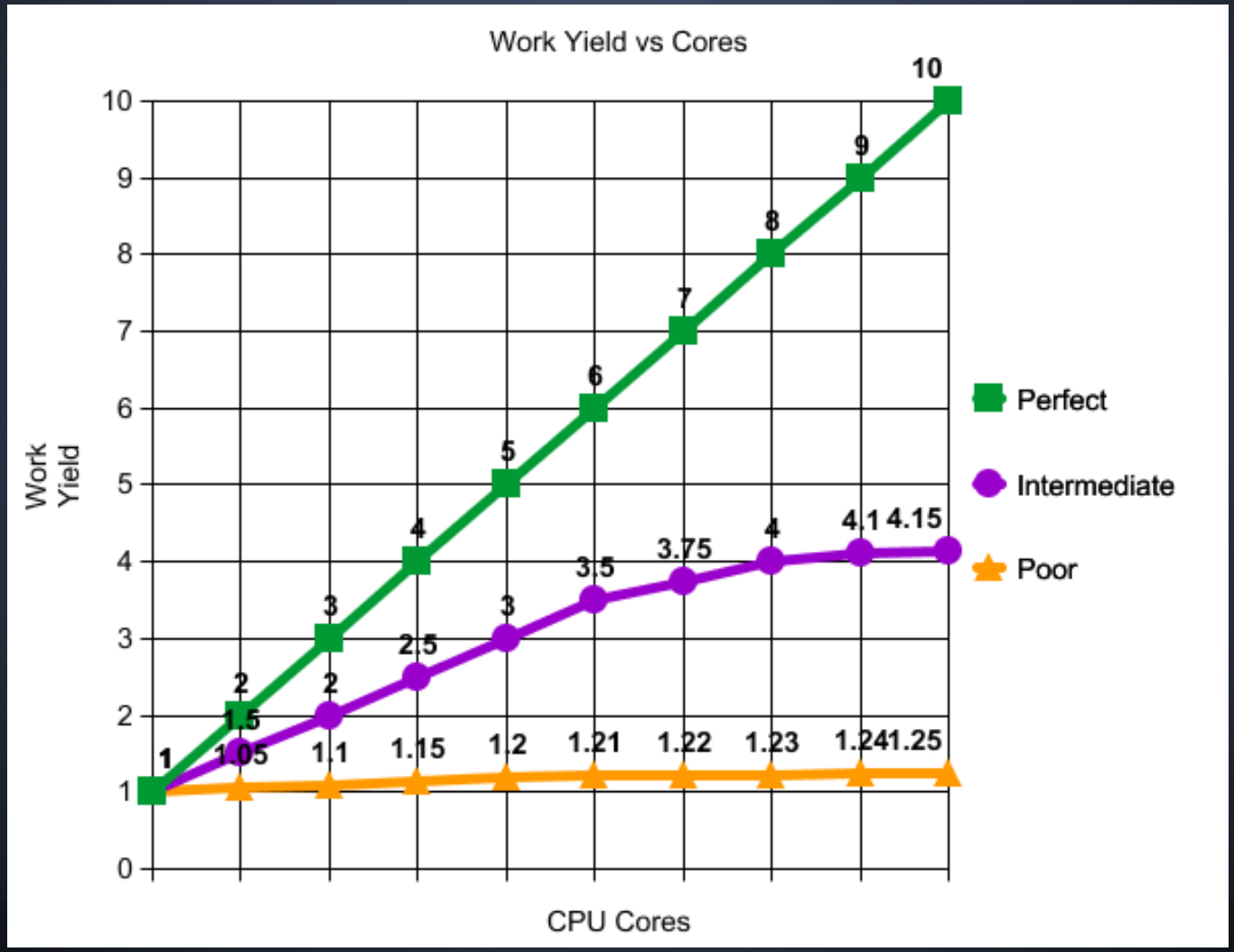
Back Track - HPC: Old School

- "Beowulf Clusters"
- Specific silos of interest:
  - academia - research
  - biotech - (Sequence analysis, Drug Discovery)
  - petrochemical (3d section / seismic data processing)
  - insurance - forecasting (what if ... probability: outcomes)
  - people with *serious* data processing need




Public (Corporate) Networking
Highly Available Databases
Private Networking
Storage
e-mail
Active Directory
System Center
Workstation
Public Network
Clustered SQL Server Databases
Head node
Failover Head node
MS-MPI Network
Private Network
Compute Nodes
Highly Available Head Node

HPC - "Work Suitability" profiles



HPC Old School - Typical Outcomes

- hardware costs
- installation services
- maintenance
- (lots of moving parts)
- food & water
- (aka power & cooling)
- lessons learned:
  - cheaper than 'big iron' (mainframes or big SMP) but it isn't 'free' and certainly it isn't 'cheap-cheap'

Spin Forward: The search for meaning

Spin Forward: The search for meaning

Spin Forward: The search for meaning

GPU: Poor man (Smart Man) HPC

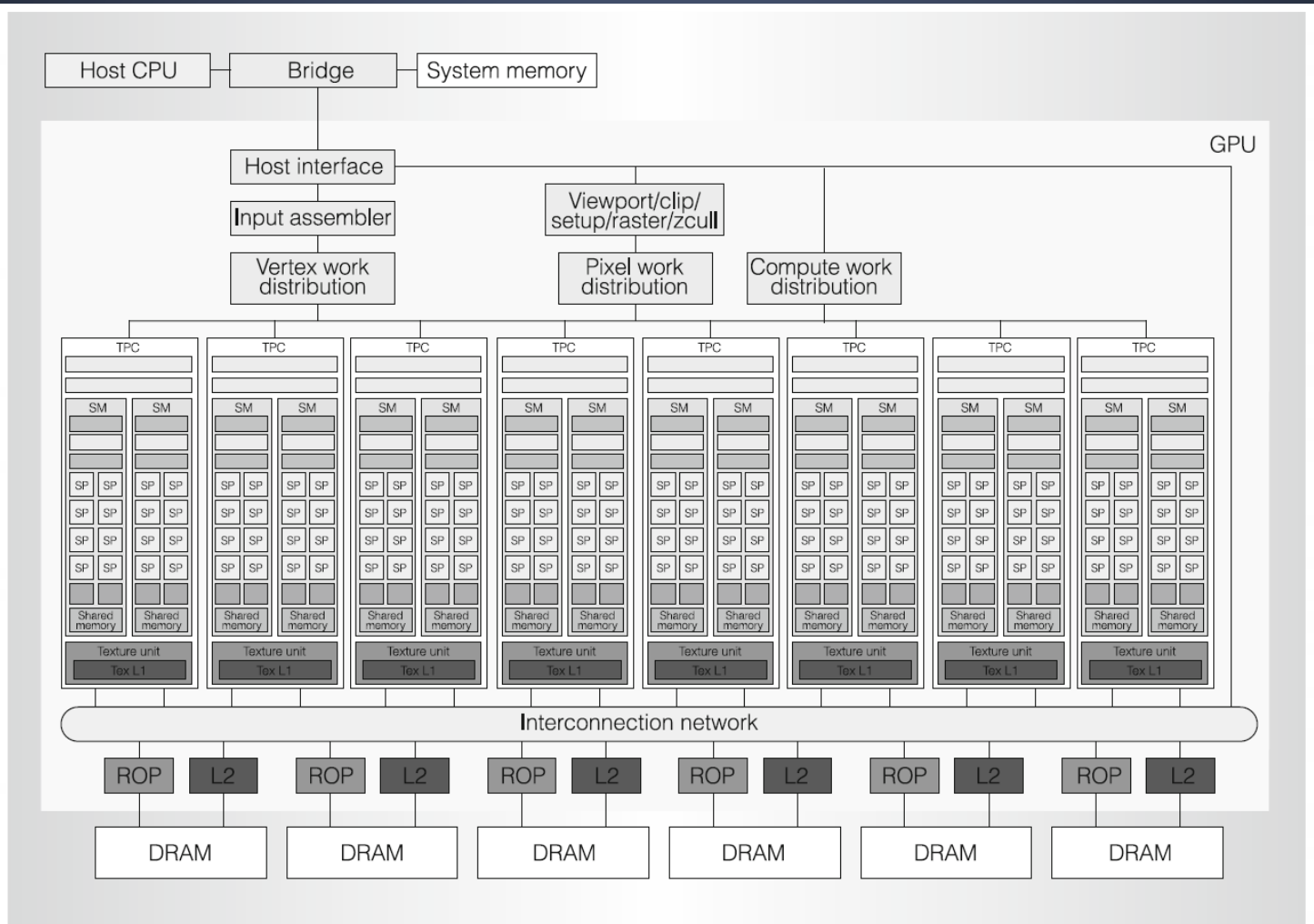


Figure 1. Tesla unified graphics and computing GPU architecture. TPC: texture/processor cluster; SM: streaming multiprocessor; SP: streaming processor; Tex: texture, ROP: raster operation processor.

GPU: Endgame

- 8 core AMD "desktop" 3ghz CPU: $180
- 16gb "desktop" ram: $80
- Nvidia GTX 560: $200 (336 CUDA Cores)
  - get a second one in there if you want - only $200 more!
- The other bits: ~misc $100's (MB, Case, PSU)
- Endpoint:
  - 8-way SMP that would have cost >$50k 10 years ago
  - GPU 'coprocessor' that would have cost >$100k 10 years ago
- Note: ATI "Stream" GPU ~ equally (or more) suitable for this use.

GPU "properly"

HPC (GPU included) - "the hard part"

- Software (design)
- Software (implementation)
- Software (integration with workflow)

(plus: suitable hardware; testing; iterative dev:optimization cycle...)

General suitability for HPC

- many (! MANY !) small to modest tasks, all independent, managed via queue manager; batch processing
- and / or: difficult (DIFFICULT) tasks - but which can be subdivided logically
  - divide and conquer: matrices, 'embarassingly parallel problems' and the like
  - HPC -> MPI; other software layers.. including CUDA
  - CUDA - Nvidia HPC library tool set for GPGPU

Putting the bits together

Putting the bits together

- Brute force password cracking:
  - WPA cracking
  - Encrypted Archive cracking
- CUDA install is well supported on BT5
- Add-in tools available to play with:
  - CUDA MultiForcer
  - cRARk
  - AirCrackNG & pyrit - WPA keys

Putting the bits together

- Encryption - is a lot cheaper to crack via brute force based approaches than it was in the past
- Rainbow tables and other 'smart' pre-compute / shared compute resources - help further reduce the 'illusion of perfect security' provided by 'large key encryption'
- Effective security architecture - needs to keep these considerations in mind.

putting the bits together

(Walk through of BT5 CUDA PDF - if time - here ?)

http://www.backtrack-linux.org/documents/BACKTRACK_CUDA_v2.0.pdf

http://www.backtrack-linux.org/wiki/index.php/CUDA_On_BackTrack

Take Home Lessons

- poor passwords are worse than no passwords (provide false sense of security which is non existent)

- well chosen, longer passwords are far (!) harder to brute force crack
- brute force cracking capacity has been rising steadily in the last ~decade and shows no sign of slowing

Take Home: Next Steps?

- NEVER played with password audit? Download "OphCrack" LiveCD (Rainbow tables based)

  http://ophcrack.sourceforge.net/

- Systems Admins? Run a 'friendly' password security audit. Be ready to rap knuckles when you find such imaginative passwords as 'password', 'kittycat', and 'moonbeam'

- Owner of a 'vaguely recent desktop system' with a dedicated GPU? You really should consider spending a 'fun evening' taking BT5 with GPU for a test-drive

Take Home: Next Steps?

- Lots of great reading, tutorials, material available online on this topic. See references at the end of the slide stack for more info.

Thanks!

- your attention is appreciated
- HASK - for being here
- HASK sponsors - for being here!

questions (comments, etc) ?

References & Interesting Reading (1/2)

http://whitepixel.zorinaq.com/

WhitePixel - Open source (GPU-accelerated password hash auditing software for AMD/ATI graphics cards.

Cracking Truecrypt encrypted disk volumes / GPU accelerated

http://code.google.com/p/truecrack/

Homepage & usage for cRARk:

http://www.crark.net/cRARk.html

General purpose hashed password cracking with GPU acceleration:

http://hashcat.net/oclhashcat-plus/

Nice review of WPA Cracking with BT5:

http://adaywithtape.blogspot.ca/2012/02/wpa-cracking-with-oclhashcat-plus.html

References & Interesting Reading (2/2)

WPS cracking of 'any vulnerable WPA protected network' in <10 hours

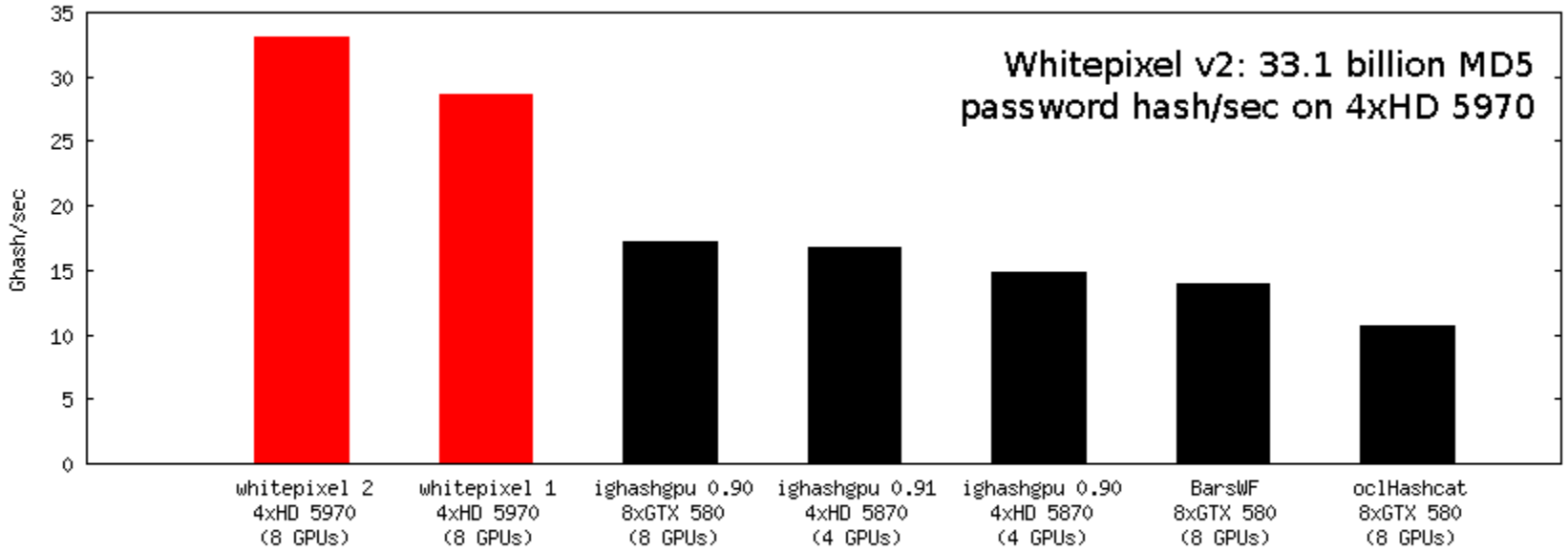
"When poor design meets poor implementation"

http://code.google.com/p/reaver-wps/
as per
http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

Whitepixel password hashing perf.

Performance

Below: performance comparison against various tools with as many of the fastest GPUs they each support.



- whitepixel 2 with "-ec all": 4xHD 5970: 33100 Mhash/sec
- whitepixel 1: 4xHD 5970: 28630 Mhash/sec
- ighashgpu 0.91.17.1 with "-t:md5 -c:a -min:8 -max:8": 4xHD 5870: 16800 Mhash/sec
- ighashgpu 0.90.17.3 with "-t:md5 -c:a -min:8 -max:8": 8xGTX 580: 17200 Mhash/sec (estimated), 4xHD 5870: 14800 Mhash/sec
- BarsWF CUDA v0.B or AMD Brook 0.9b with "-c 0aA~ -min_len 8:": 8xGTX 580: 13920 Mhash/sec (estimated)
- oclHashCat 0.23 with "-n 160 --gpu-loops 1024 -m 0 '?1?1?1?1' '?1?1?1?1'": 8xGTX 580: 10720 Mhash/sec (estimated)

RAR Password Hashing - Relative Perf#s

Chart with RAR 3.x performance for password length == 4.