ELCOMSOFT
PROACTIVE SOFTWARE

Modern Password Recovery: GPUs and Supercomputers

Andrey Belenko (a.belenko@elcomsoft.com)
ElcomSoft Co. Ltd.

Halle **B3** Stand **614**

Our Solutions

- Advanced Office Password Recovery
  - Microsoft Office, all versions
- Advanced PDF Password Recovery
  - Adobe PDF, all versions
- Advanced EFS Data Recovery
  - Decrypt files encrypted with EFS
- Elcomsoft System Recovery
  - Regain access to Windows
- Distributed Password Recovery
  - Distribute password recovery among many computers

Why recover the password?

- You might forgot one
- Your employee might forgot one
  - or just telling that he did after you've fired him
- You might perform security audit
- You might perform forensic investigation
  - or you just work for the government

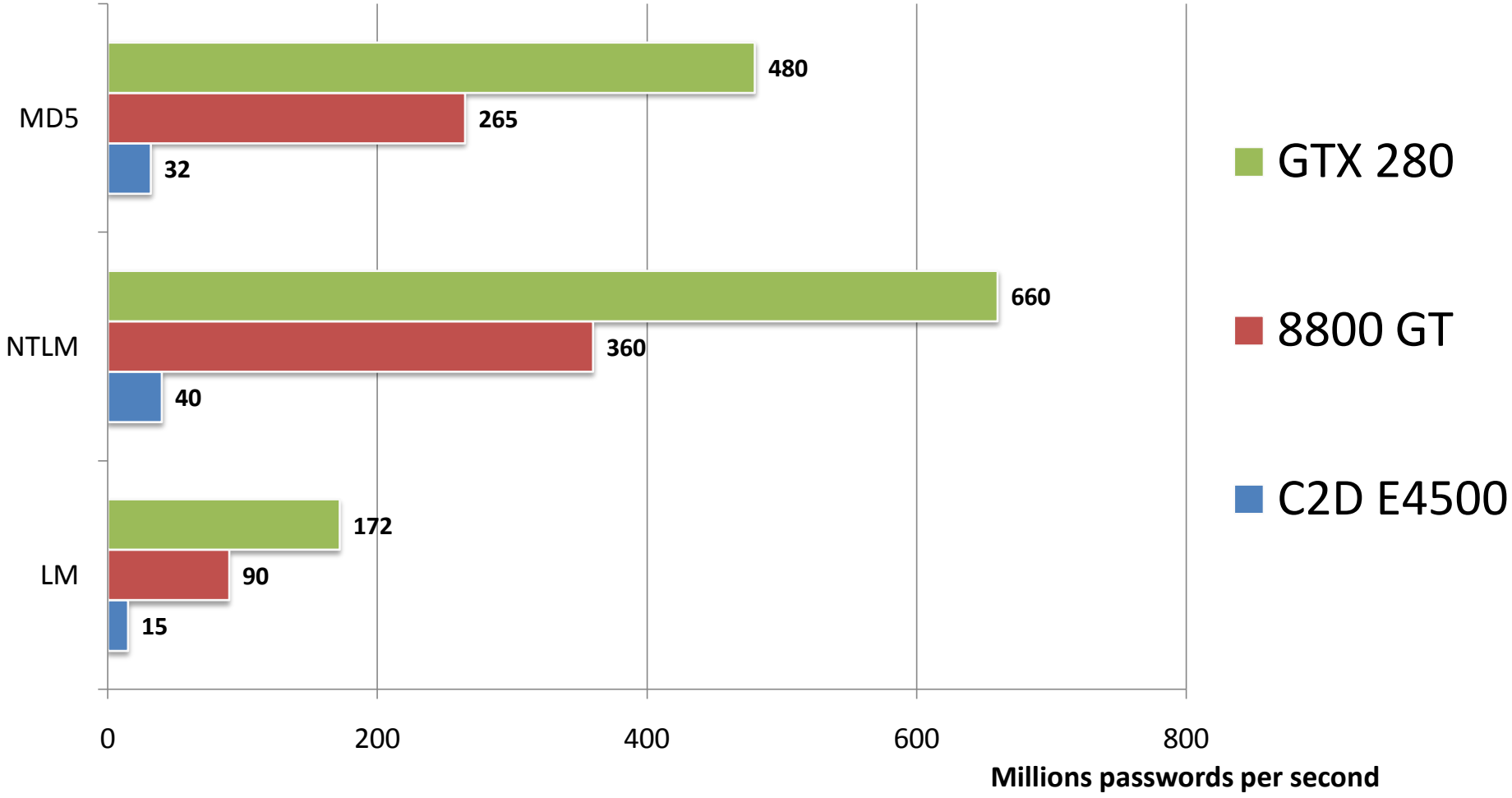
Stronger the password sooner you'll need to recover it ☺

Why CPU is not enough?

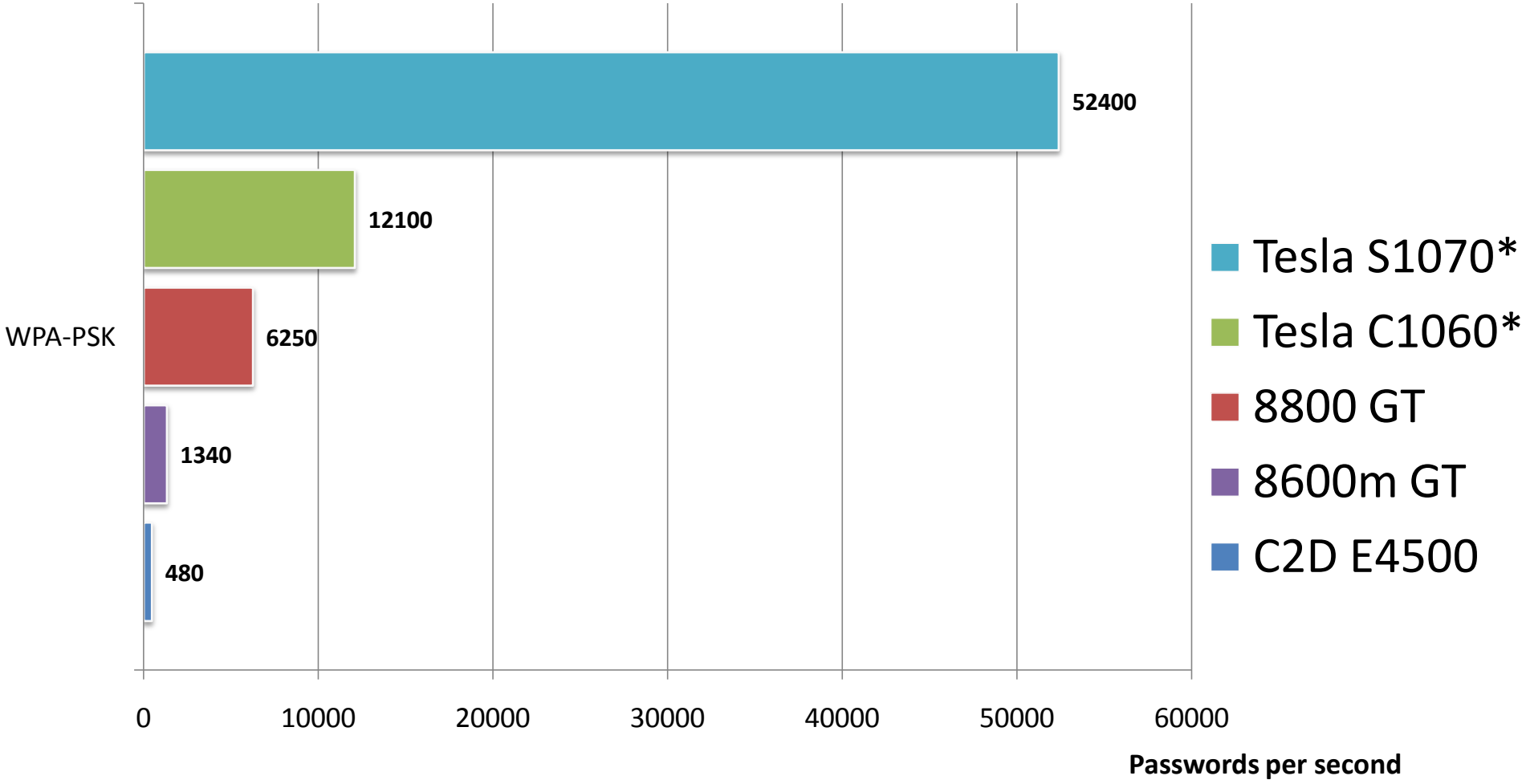
- Password audit requires much computations
  - they are usually simple but repeated billion times
- CPUs are not effective with such workload
  - just because they are not designed to
  - …but MMX and SSE change this a bit
- GPUs are effective with repeating computations
  - but they lack other features, so you can't port Linux to GPU ☺

With GPU you can do it in less time and money

What's the difference?



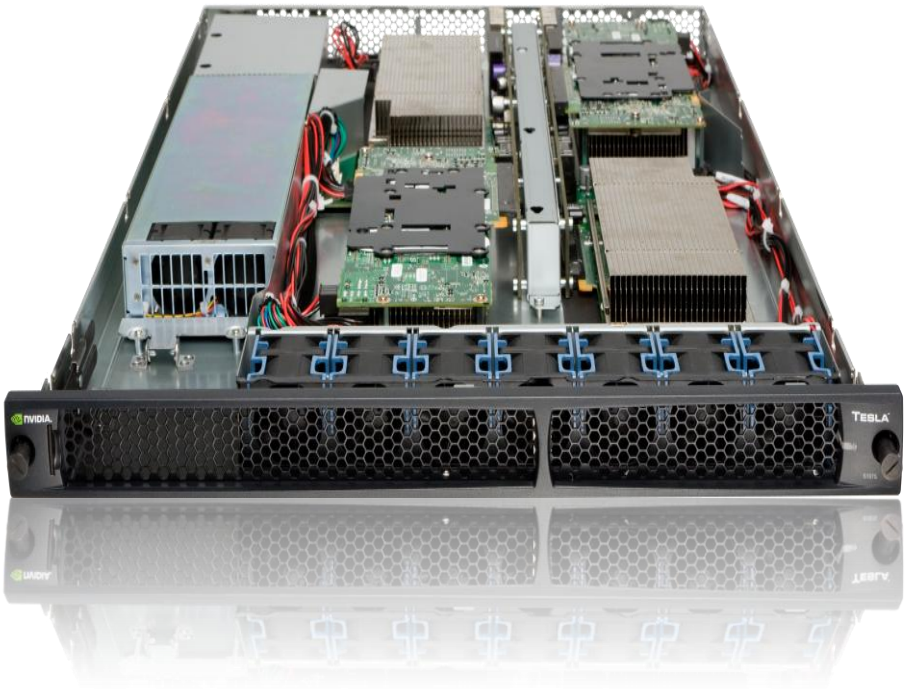
What's the difference?



Tesla C1060 Computing Processor

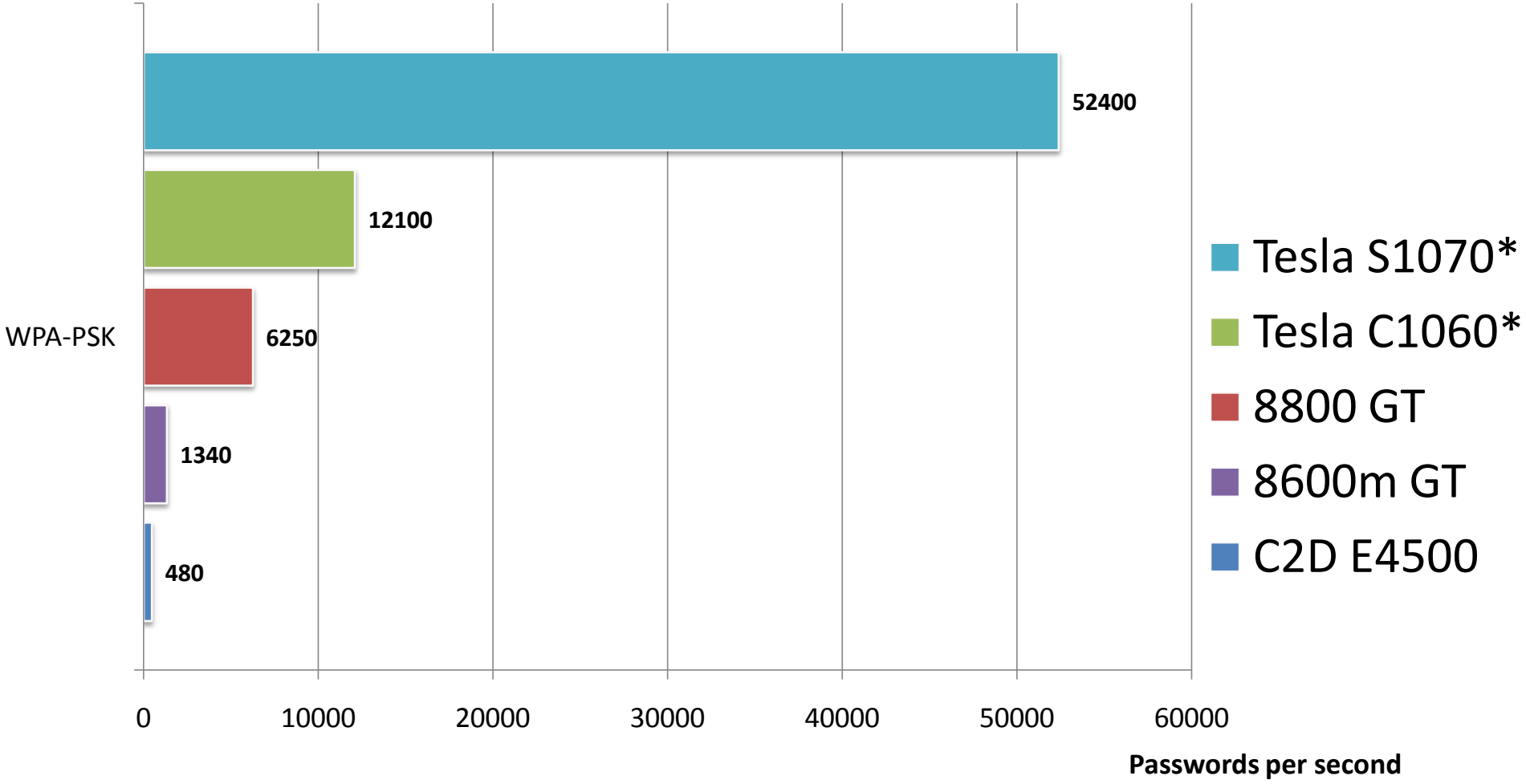
Processor	1 x Tesla T10
Number of cores	240
Core Clock	1.33 GHz
On-board memory	4.0 GB
Memory bandwidth	102 GB/sec peak
Memory I/O	512-bit, 800MHz GDDR3
Form factor	Full ATX: 4.736” x 10.5” Dual slot wide
System I/O	PCIe x16 Gen2
Typical power	160 W

Tesla S1070 1U System



Processors	**4 x Tesla T10**
Number of cores	**960**
Core Clock	**1.44 GHz**
Performance	**4 Teraflops**
Total system memory	**16.0 GB (4.0 GB per T10)**
Memory bandwidth	**408 GB/sec peak (102 GB/sec per T10)**
Memory I/O	**2048-bit, 800MHz GDDR3 (512-bit per T10)**
Form factor	**1U (EIA 19" rack)**
System I/O	**2 PCIe x16 Gen2**
Typical power	**700 W**

What's the difference?



Low-Budget Supercomputer

Part	Price	Quantity	Total
700W+ PSU	€120	1	€120
X38/X48 Motherboard	€170	1	€170
Intel Core 2 Quad Q8200	€180	1	€180
2x2Gb RAM	€25	2	€50
400Gb HDD	€50	1	€50
2x NVIDIA 9800GX2	€400	2	€800
Total:			**€1370**

Expected performance:

- MD5 — 1200M pass/sec
- NTLM — 1600M pass/sec
- LM — 420M pass/sec

ELCOMSOFT
PROACTIVE SOFTWARE

Modern Password Recovery: GPUs and Supercomputers

Andrey Belenko (a.belenko@elcomsoft.com)
ElcomSoft Co. Ltd.

Halle **B3** Stand **614**