ELCOMSOFT
PROACTIVE SOFTWARE

Breakthrough in Password Recovery: Thunder Tables and GPUs

Andrey Belenko (a.belenko@elcomsoft.com)

ElcomSoft Co. Ltd.

Hall **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

Security is improving

Changes in past five years:

- Password recovery became slower
- «Salting» used to avoid pre-computations
- (Much) Stronger cryptography is used

What can be done?

- **Increase password recovery speed**
- **Continue research**

Our Research

- Intuit Quicken backdoor
  - Involved factoring RSA key
- Advanced Rainbow Tables
  - ***Guaranteed*** almost instant decryption
- Using GPUs to accelerate password recovery
  - ***25x speedup*** with generally available hardware

Attack Alternatives

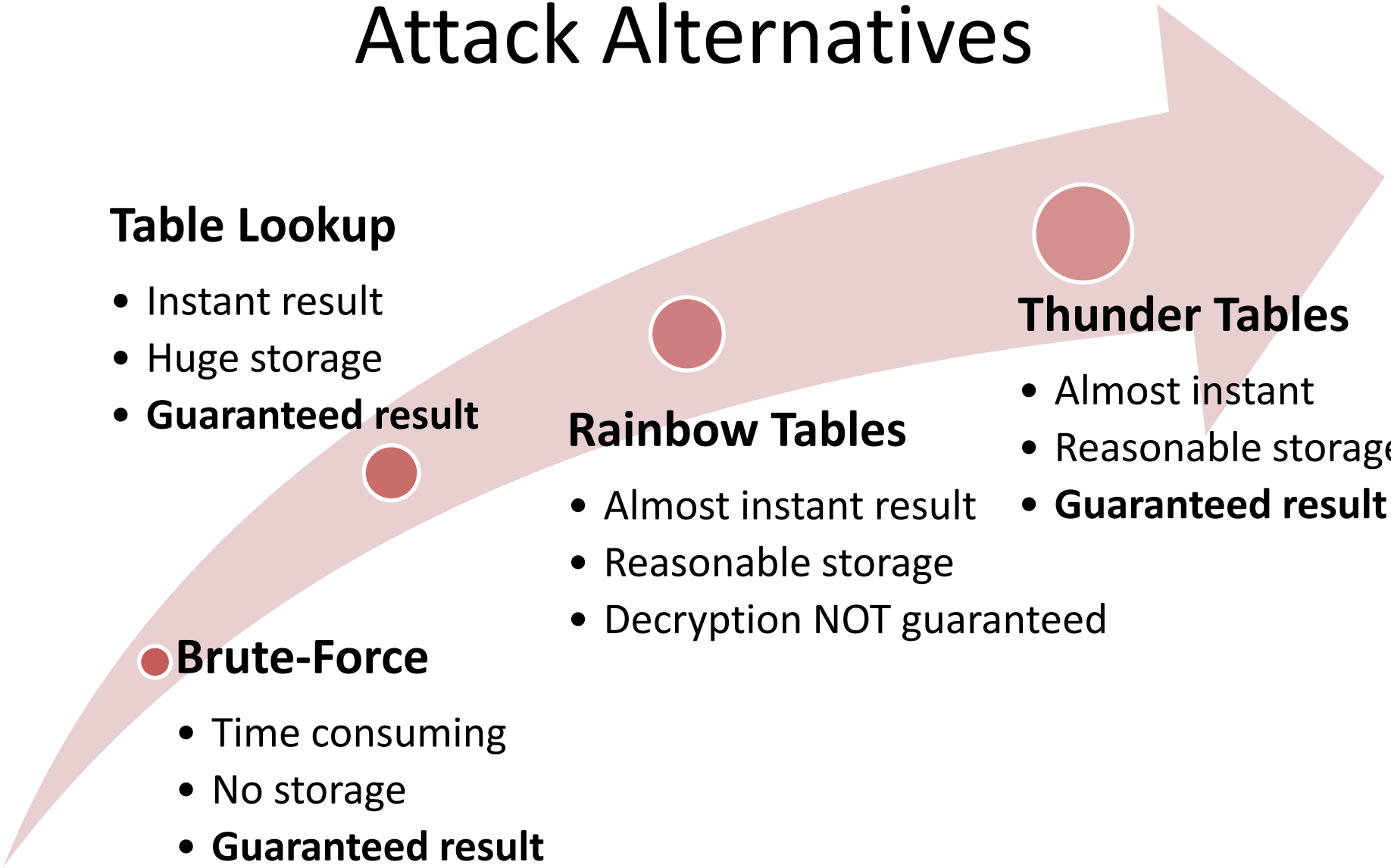


Table Lookup

- Instant result
- Huge storage
- **Guaranteed result**

Brute-Force

- Time consuming
- No storage
- **Guaranteed result**

Rainbow Tables

- Almost instant result
- Reasonable storage
- Decryption NOT guaranteed

Thunder Tables

- Almost instant
- Reasonable storage
- **Guaranteed result**

Thunder Tables

Table 1

Table 2

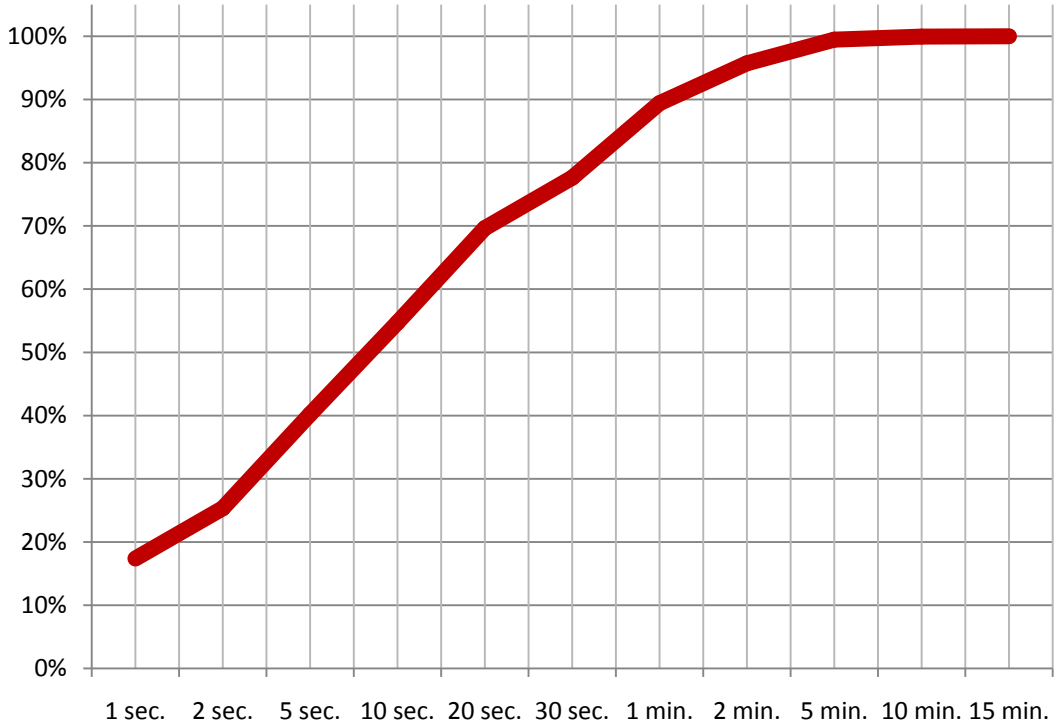
Table 3

Total coverage:

If attack fails, check ONLY keys NOT COVERED by tables

Thunder Tables: Performance

% Keys Recovered	Elapsed Time
50%	8 sec.
90%	1 min.
95%	2 min.
99%	4 min.
100%	13 min.



Average attack time is 25 sec.

* Test configuration: Intel Core 2 Duo 1.86 GHz with 1 Gb RAM

Password Recovery: How to do it **Faster**?

Software Optimization	• Free for End-Users • Limited speedup (10-20%) • Need to re-optimize for every new CPU
Special Hardware	• Expensive devices • Won't work with software from other vendors • Not very cost-effective
Common Hardware	• Hardware already installed in many computers • Cost-effective • Compatible with software from different vendors • Can be used for other applications

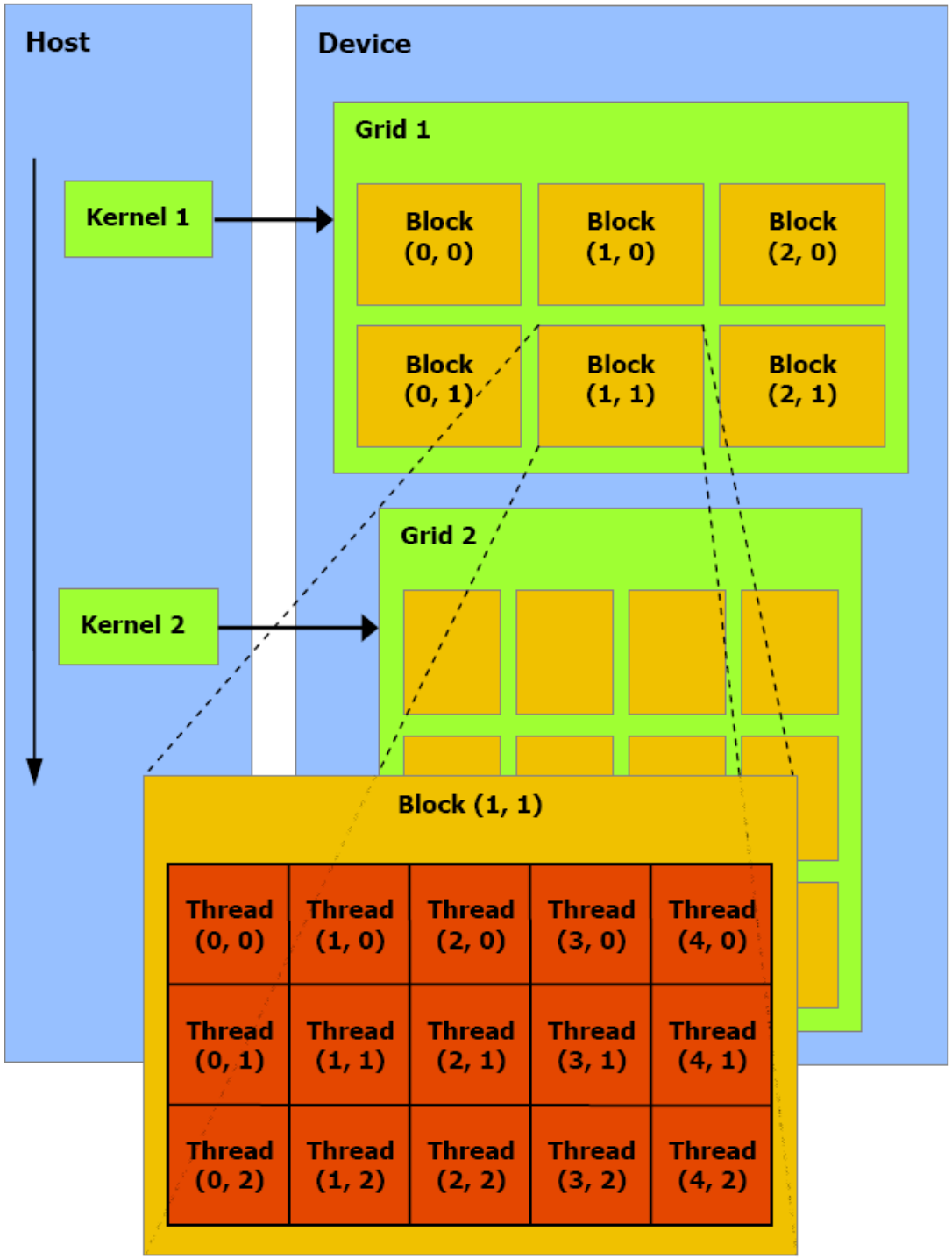
GPU: Basics (NVIDIA GeForce8)

- Display adapter acts as co-processor for CPU
  - Up to 128 processors on board
  - Up to 1.5 Gb memory on board
  - Up to 4 boards in one computer
- C-like programming language for writing GPU code
- New programming model

GPU: Programming Model

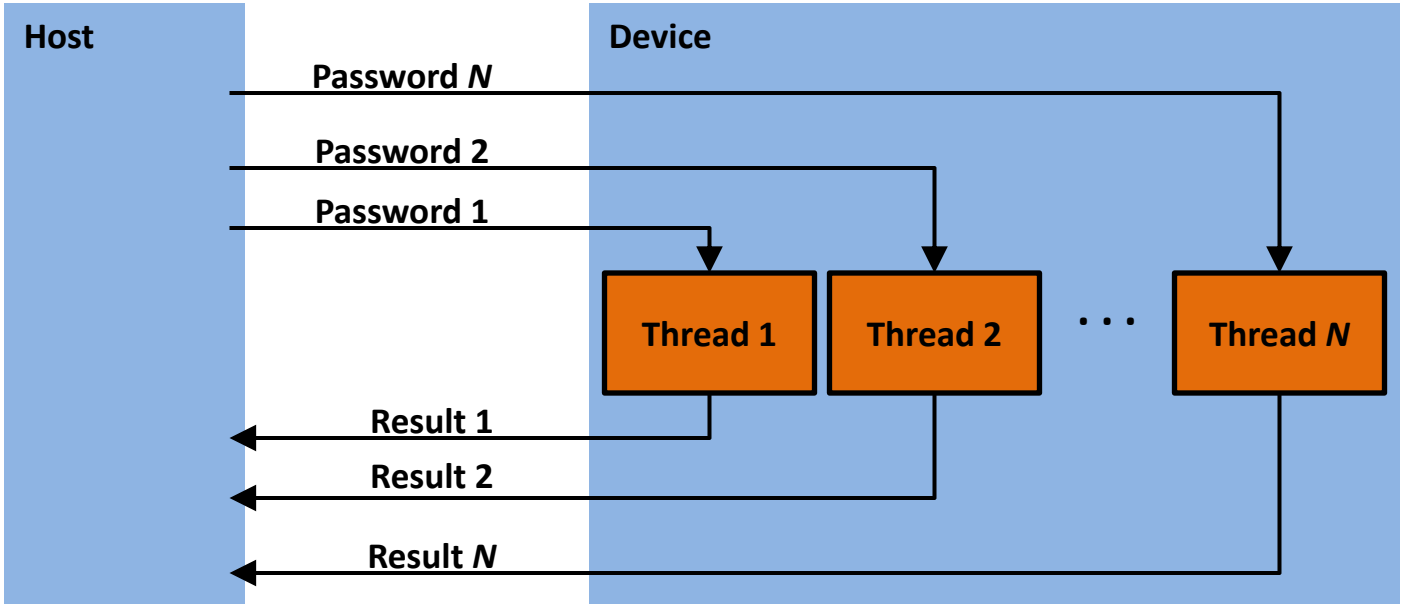
- Data-parallel portions of application are executed on GPU
  - Function compiled for GPU is called ***kernel***
- Kernel runs as a batch of threads
  - Threads are organized as a grid of thread blocks
- All threads run same code on different data

- Blocks are 3D arrays of threads
- Grid is 2D array of blocks
- Hardware allows up to 2^{41} threads

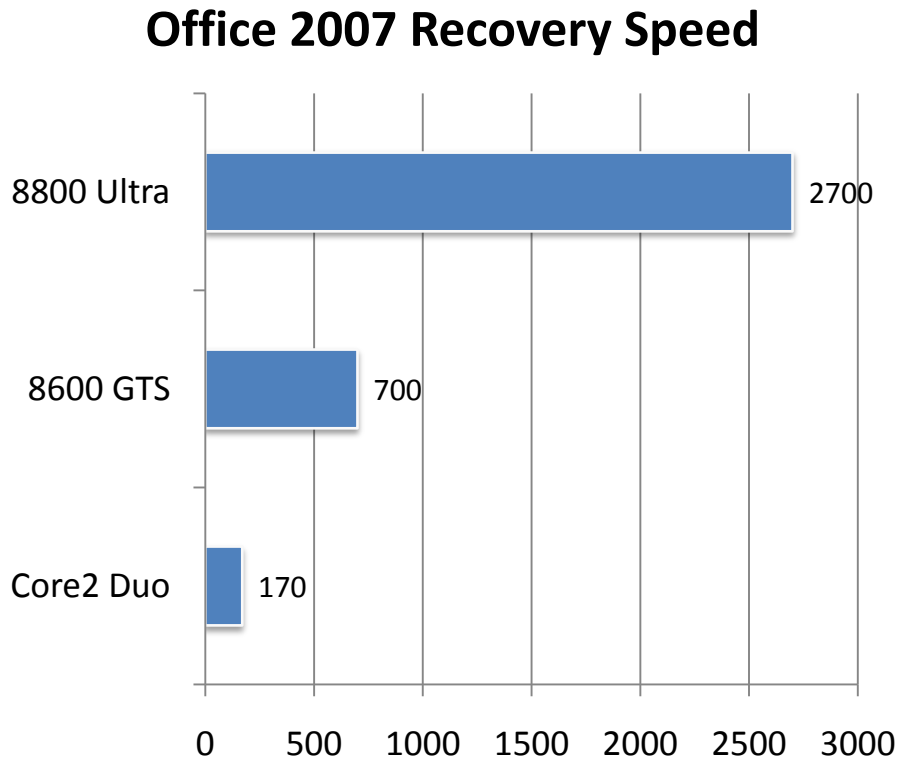


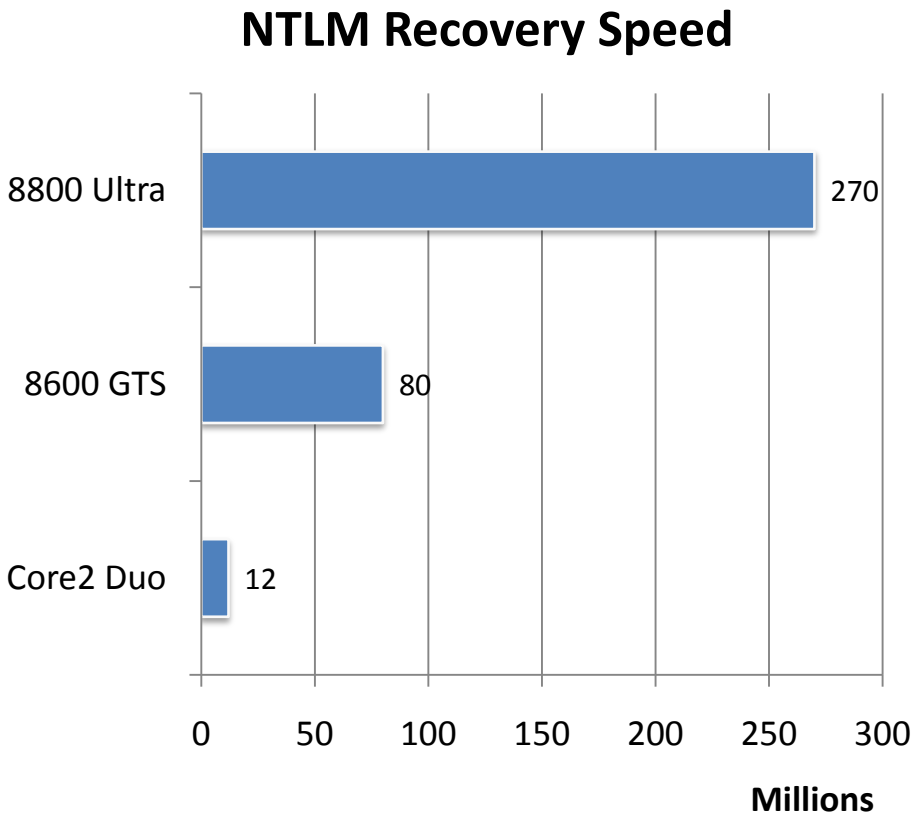
GPU: Password Recovery

- Fits well to new programming model
- ***N*** threads check ***N*** password in parallel
- No inter-thread communications



GPU: Performance





Coming soon: PGP, RAR, LM and more…

ELCOMSOFT
PROACTIVE SOFTWARE

Breakthrough in Password Recovery: Thunder Tables and GPUs

Andrey Belenko (a.belenko@elcomsoft.com)

ElcomSoft Co. Ltd.

Hall **B3** Stand **614**