Luca Vaccaro
http://code.google.com/p/truecrack/
luck87@gmail.com

TrueCrack
Password cracking for TrueCrypt© volume files.

User development guide.

Introduction

- TrueCrypt ©
  - software application used for on-the-fly encryption (OTFE).
- TrueCrack
  - bruteforce password cracker for TrueCrypt © (Copyrigth) volume files, optimazed with Nvidia Cuda technology.
  - This software is Based on TrueCrypt, freely available athttp://www.truecrypt.org/

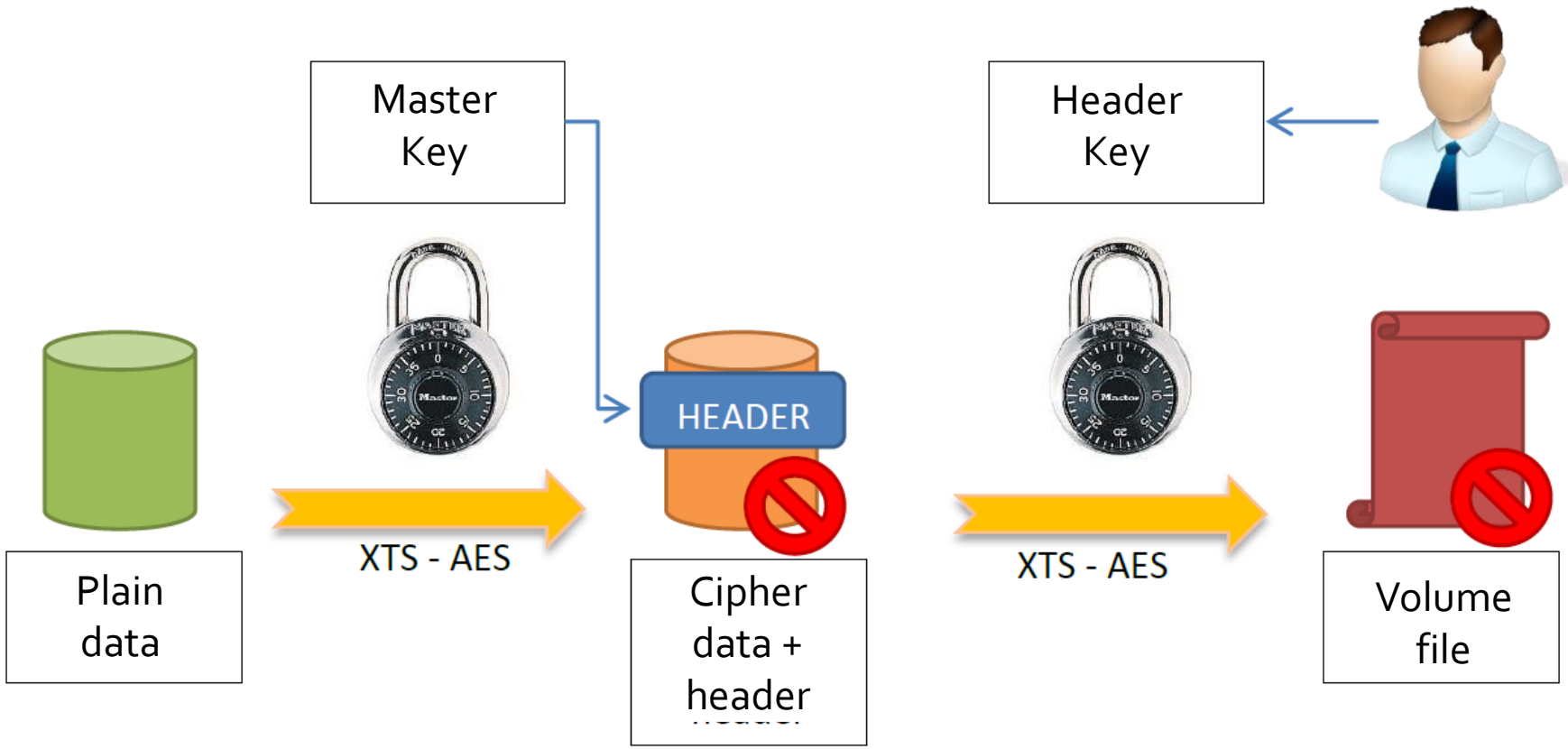
TrueCrypt©: keys

- Master key
  - Crypt the volume of data.
  - Generated one time in the volume creation phase from random value.
  - Write inside the header section of the volume file.
- Header key
  - Crypt the header section of the volume file.
  - Generated from a user password and a random salt (64 bytes).
  - The salt is write in plain text in the first 64 bytes of volume file.

TrueCrypt©: algoritms

- Hard disk encryption:
  - Standard block cipher: XTS
  - Hash availables: AES, Serpent, Twofish
  - Default: AES
- Key derivation function:
  - Standard algorithm: PBKDF2
  - Hash availables: RIPEMD160, SHA-512, Whirpool
  - Default: RIPEMD160

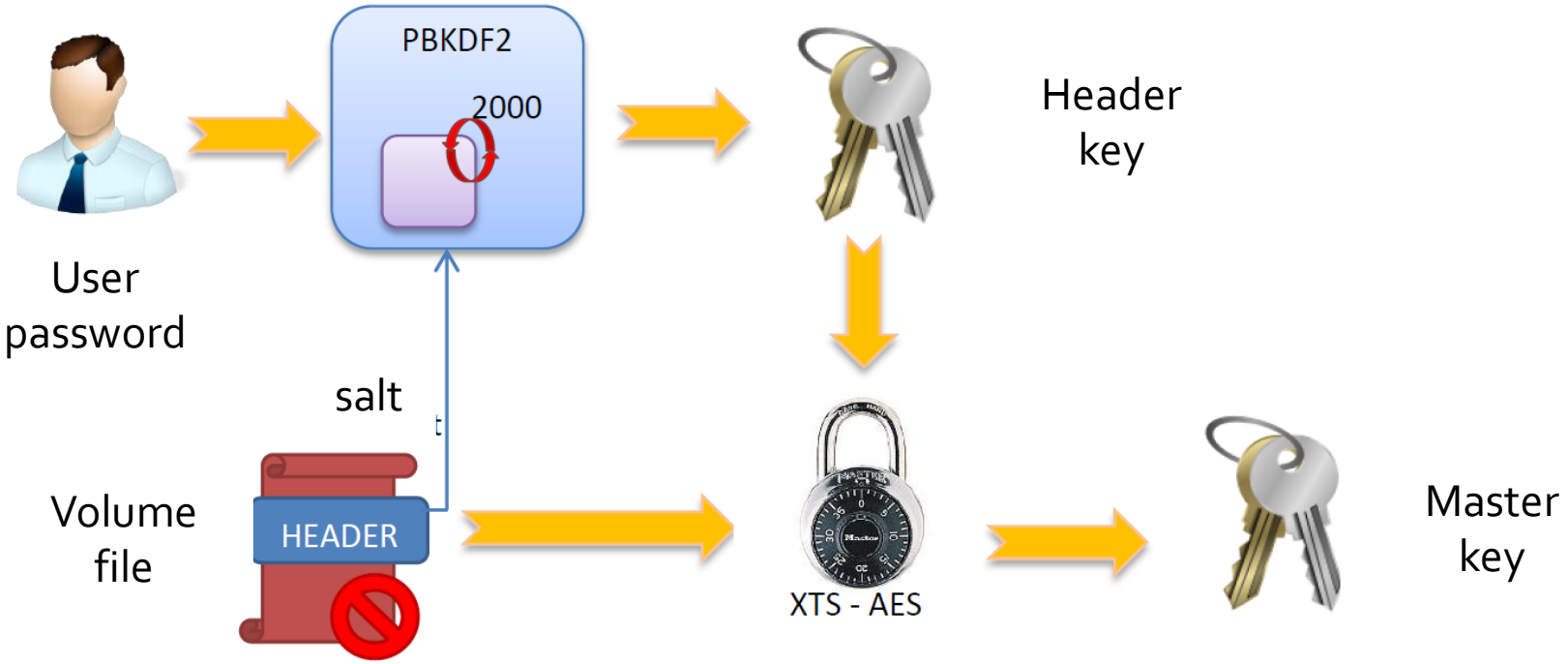
TrueCrypt©: cipher



TrueCrypt©: decipher/1

- Opening a TrueCrypt volume means to retrieve the Master Key from the Header section
- In the Header there are some fields (true, crc32) for checking the success of the decipher operation
  - If the password is right or wrong

TrueCrypt©: decipher/2

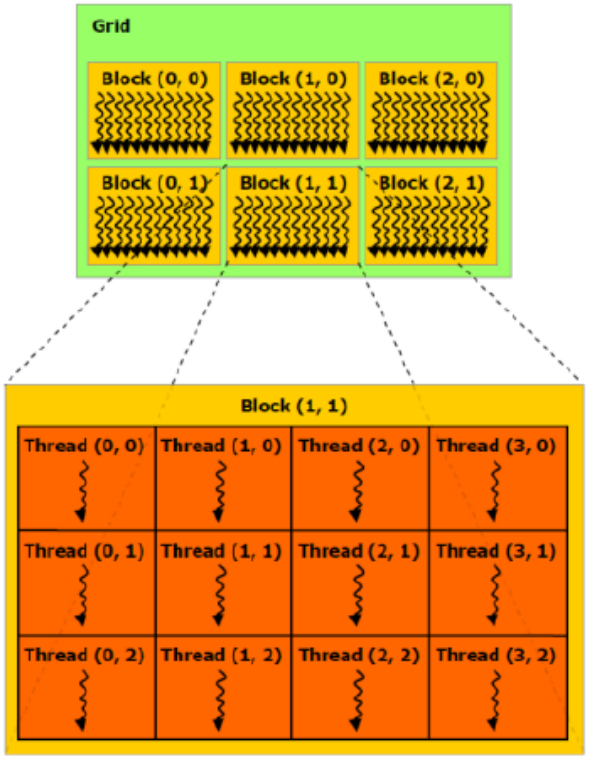


CUDA: introduction

- **CUDA** or **Compute Unified Device Architecture** is a parallel computing architecture developed by Nvidia.
- CUDA gives developers access to the virtual instruction set and memory of the parallel computational elements in CUDA GPUs.

CUDA: computation

- Each GPU is a collection of multicores. Each core can run mmore cuda «block», and each block can run a numbers of parallel «thread»



1. Level of parallilism : block
2. Level of parallelism : thread

CUDA: memories

- Global
  - global memory, without cache, access by all blocks and threads, size related to device memory.
- Shared
  - Shared memory between threads of one single block, with a cache, size related to GPU architecture.
- Local
  - Local memory of each thread, without cache, size related to GPU architecture.
- Constant
  - Constant and invariable memory, access by all blocks and threads.

TrueCrack

- TrueCrack makes a bruteforce attack to retrieve the master key of a TrueCrypt© volume.
- Modes of operations:
  - Dictionary attack: read the passwords from a file of words (one password for line).
  - Charset attack: generate the passwords from a charset of symbols defined by the user (for example: all possible strings of n characters from the charset "abc").

TrueCrack: limit

- The current implementation work in the following conditions:
  - Key derivation function:

    PBKDF2 - RIPEMD160.
  - Hard disk encryption block cipher mode:

    XTS - AES.
  - TrueCrypt volume:
    not hidden partition and inside one single file.

TrueCrack: implementation

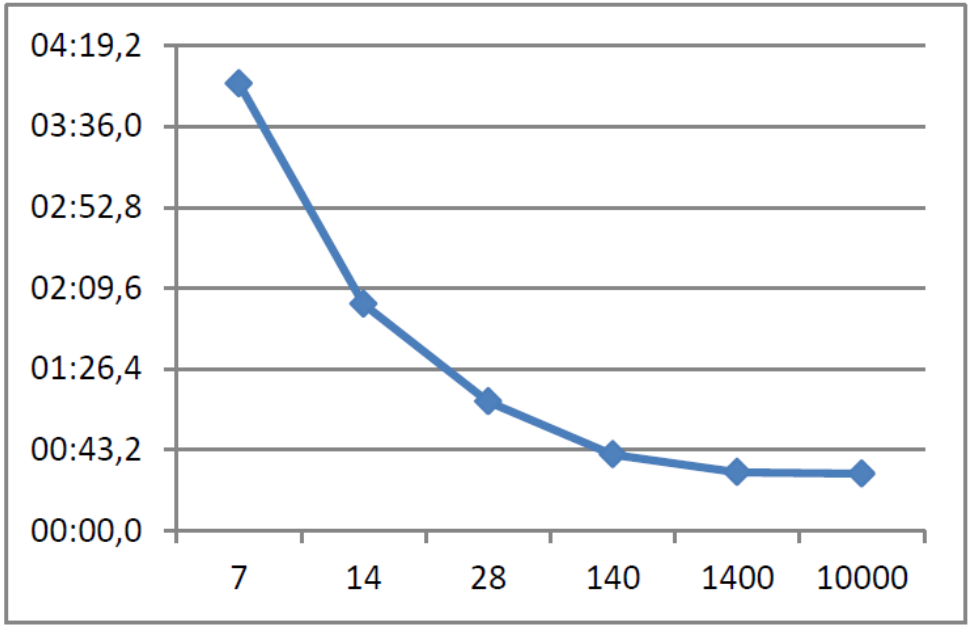
- TrueCrack works with CUDA:
  - The software test more passwords in parallel.
  - Each CUDA block check and verify a single word
  - The threads for each CUDA block:
    - 10 threads (parallel) computed the PBKDF2-RIPEMD160 algorithm to derive the header key.
    - 1 threads (sequential) computed the cipher XTS-AES from header key and check the success of the decipher operation.

TrueCrack: perfomance/1

- Test environment:
  - CPU mode
    - System: Intel Core-i7 920, 2,67GHz
    - Dictionary: 10,000 words
    - Average length of word: 10 characters
    - Total time: 11m 01,1s
  - GPU mode
    - Board: nVidia GeForce GTX470
    - Multiprocessor unit: 14
    - Core CUDA: 448
    - Clock processor/shader: 607/1215 MHz

TrueCrack: perfomance/2

Total execution time for a dictionary attack of 10,000 words in the GPU test. The CPU takes: 11m 01,1s.

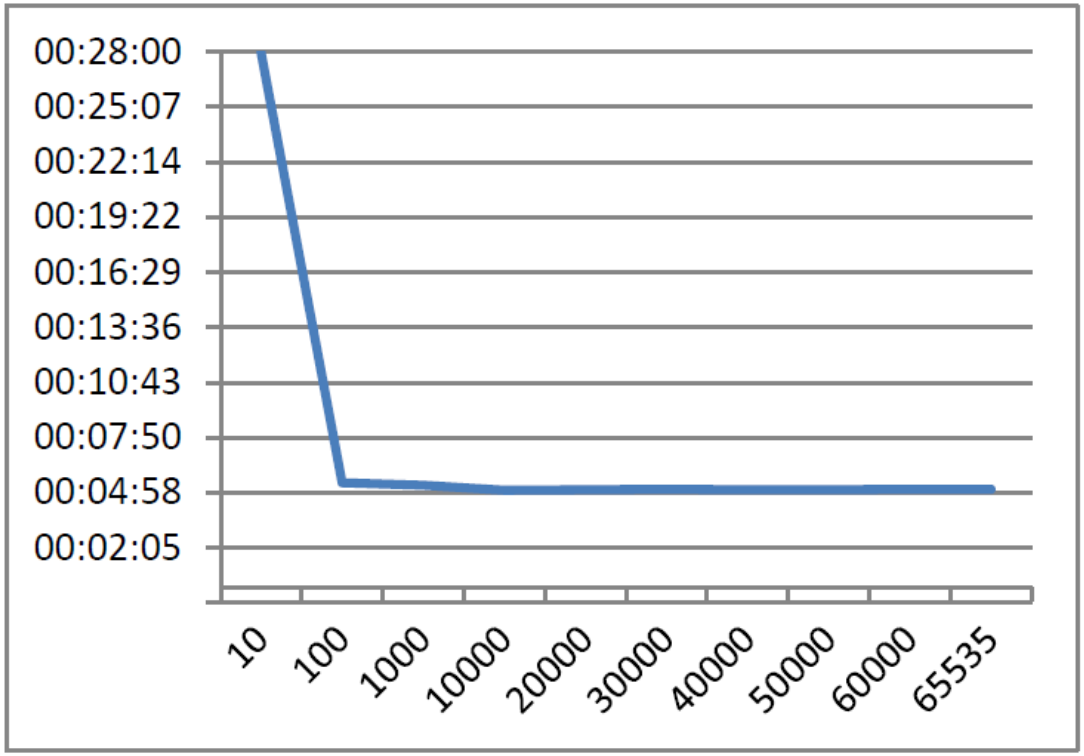


Parallel Blocks	GPU
7	3m 58,919s
14	2m 1,170s
28	1m 8,915s
140	0m 40,691s
1'400	0m 31,234s
10'000	0m 30,425s

Where 14 is the number of multiprocessor cores of GTX 470 board .

TrueCrack: perfomance/3

Total execution time for a dictionary attack of 100,000 words in the GPU test with different number of parallel blocks.



Parallel Blocks	GPU
10	27m 59,839s
100	5m 27,976s
1'000	5m 19,936s
10'000	5m 4,465s
20'000	5m 6,977s
30'000	5m 7,319s
40'000	5m 6,353s
50'000	5m 5,629s
60'000	5m 7,540s
65'535	5m 7,200s