DeepSec 2017 Talk: BitCracker – BitLocker Meets GPUs – Elena Agostini

Posted on **October 25,2017** by **sanna**

Encryption and ways to break it go hand in hand. When it comes to the digital world, the method of rapidly using different keys may lead to success, provided you have sufficient computing power. The graphics processing units (GPUs) have come a long way from just preparing the bits to be sent to the display device. Nowadays GPUs are used for a lot of computational expensive tasks. At DeepSec 2017 you will hear about keys, encryption, and storage encryption – all with the use of GPUs, but forthe purpose of cracking keys.

BitLocker (formerly BitLocker Drive Encryption) is a full-disk encryption feature available in recent Windows OS (Vista, 7, 8.1 and 10). It is designed to protect data by providing encryption for several types of memory units like internal hard disks or external removable memory devices (BitLocker To Go feature), offering a number of different authentication methods, like Trusted Platform Module, Smart Key, Recovery Key, password, and the like.

During this talk Elena will describe how the password authentication method works and the algorithms used during the decryption procedure; she'll give an insight into the complex architecture of BitLocker's keys, analyzing BDE format and metadata structures of an encrypted volume.

Finally Elena will present BitCracker, that is the first open source password cracking tool for memory units encrypted with BitLocker using the password authentication method. It aims at finding the right password doing a dictionary attack by means of GPUs. BitCracker is able to process up to 1400 passwords/second (about 2.900.000.000 SHA-256/second) on a NVIDIA GPU Tesla P100.

Currently, BitCracker is theOpenCL BitLocker format of John the Ripper, but there is also astandalone CUDA implementation available.

Elena Agostini received her PhD in Computer Science from the University of Rome "La Sapienza" in collaboration with the National Research Council of Italy. The main topics of her research are GPUs used both for cryptanalysis or communications and wireless network protocols.

Massimo Bernaschi is the second author of the talk Elena is going to present at DeepSec. He has been 10 years with IBM working in High Performance Computing. Currently he is with the National Research Council of Italy (CNR) as Chief Technology Officer of the Institute for Computing Applications. He is also an adjunct professor of Computer Science at "Sapienza" University in Rome.

Posted in:Conference | Tagged:Authentication,BitCracker,BitLocker,Crypto,DeepSec,Talk | With 0 comments