GPGPU Acceleration of Cryptographic Applications

Giovanni Agosta, Alessandro Bareghi, Fabrizio De Santis, Andrea Di Biagio
Politecnico di Milano
{agosta,bareghi,di biagio}@elet.polimi.it, fabrizio.desantis@mail.polimi.it

Gerardo Pelosi
Università degli Studi di Bergamo
gerardo.pelosi@unibg.it

I. OVERVIEW

Cryptographic algorithms are crucial to the security of modern computing systems. The peculiar nature of such algorithms leads them to be computationally intensive by design. Speeding up cryptographic algorithms through parallelization can therefore prove effective especially when large amount of data are to be encrypted. At the same time, massive amounts of SIMD-like parallel computational power can speed up the breaking of cryptographic algorithms.

In both cases, we show that software solutions targeting GPGPU devices can compete with dedicated hardware solutions on a performance/cost metric. To prove this, we provide two case studies: the breaking of the well-known DES algorithm, comparing a NVidia G200-based solution to the Copacobana FPGA-based solution; and disk volume encryption by means of the TrueCrypt suite, targeting both the Serpent and Twofish algorithms in the XTS mode of operation.

In both cases, we show how to correctly tune the design parameters, including data allocation, thread packing, and parallelization strategy. Overall, our implementation of TrueCrypt running on a NVidia GTX260 GPU outperforms by 67% the baseline implementation running on a four core CPU [2], while our implementation of DES breaking is able to find a DES key in about 18 days, at a cost equal to that of the Copacobana [3].

II. DES BREAKING

The Data Encryption Standard (DES) [11] is one of the most popular encryption algorithms, standardized by NIST in 1977 and subsequently maintained as a FIPS security primitive up to 2005 [12], when it was retired, since it had been proved that the cipher could be broken via a brute force attack [10]. Even though DES was not anymore considered safe for government applications, comments had to be addressed holding that “the DES should be retained because it is widely used in the market” and “FIPS 463” and associated standards are used in the commercial world and serve important functions, including use by the entertainment industry for real-time broadcast security, to prevent unrestricted copying of files, and for the security of digital television signals” [12]. So, while not anymore relevant for high-security applications, DES continues to be used in many commercial applications due to backward compatibility reasons, thus living long beyond its recommended lifetime. The DES encryption primitive is still supported by most encryption suites, including OpenSSL [14].

Since DES was designed specifically for highly-optimized hardware implementations, its structure contains many operations which require computationally expensive adaptations in order to be executed by a general purpose CPU. Thus, both known brute force attacks, Deep Crack [10] and COPACOBANA [6], rely on dedicated hardware designs, the first in the form of ad-hoc ASIC chips, the second in the form of FPGA-based hardware. Special purpose hardware is, however, expensive, thus DES still remains a viable solution for short-term secrets, when the potential attacker has only access to consumer hardware and lacks the technical knowledge and skills required in order to build ad-hoc cracking solutions. The goal of this paper is to explore the viability of brute force attacks to the DES cipher with consumer grade hardware, thus removing the last technical barrier left to attack the cryptosystem.

Given the amount of computation needed to mount such an attack, GPGPU boards appear as the most promising target hardware: not only these boards provide a very low cost/MIPS ratio (and one bound to drop further, given the nature of the GPU market), but they are readily available and easily programmed by anyone with general purpose programming skills.

We show that a brute force attack can be mounted against DES with today’s GPUs, even if the performances of modern dedicated hardware solutions such as COPACOBANA are not reached. The fast evolution of the GPU market will provide more and more computational power in the near future, making in the end the software solution more cost efficient than comparable hardware solutions. Moreover, since there is already a widely deployed installbase of these devices, it is easy to harness, either through explicit agreement or by taking control of common desktops, a large amount of computing devices. In particular, in the second case, typical of a botnet scenario, the legitimate owner of the hardware is not likely to discern the exploiting of its computational resources, since the brute force computation is run on the GPU, which is very often idle under a typical home workload.

III. DISK ENCRYPTION WITH TRUECRYPT

Data storage encryption has always been a key point in warranting confidentiality, but encrypting large disk volumes imposes a significant computational load on the CPUs. In case of a single host system the CPU time used for encryption is subtracted from the one available for coping with the user’s needs. On dedicated Network Area Storage managers (NAS) throughput is sacrificed in order to deal with the
additional workload due to encryption. A way to reduce this computational load is to employ dedicated ASIC coprocessors but this comes at a major cost, especially on user machines. Moreover, the accelerators must be designed according to each platform specification and are typically customized for a single encryption algorithm with fixed key sizes [8], thus resulting in a not so flexible solution.

A viable alternative comes from the Graphics Processing Unit (GPU) world where coprocessors have grown towards increasing levels of hardware parallelism, while containing the costs. Since these platforms are now supported by development toolchains which allow the implementation of general purpose software without the need of fitting through the graphics specific interface, they may be a viable choice for the implementation of generic computationally demanding algorithms. The advantage of such a choice lies in both using off-the-shelf hardware which comes at a very low cost with respect to ASIC solutions, and exploiting the already deployed installbase on common personal computers. Moreover, this design solution relies on a standard bus interface (PCI-Express) and on a subset of the recently standardized OpenCL language [9] for high performance computing on graphic hardware.

The use of GPUs to speed up the computation of cryptographic primitives was pioneered by D. Cook et al. in [5]. Further developments [7] focused on the engineering of an AES implementation oriented towards the use in SSL network communication channels, and considered the ECB, CBC and CTR modes of operation.

The goal of this work is to analyse the design and performance of a GPU-optimized implementation of a disk encryption application employing the XTS mode of operation applied together with the Twofish [13] and Serpent [4] algorithms within the well-known TrueCrypt suite [1]. The XTS mode of operation has been recognized as the standard for disk encryption, and Twofish is commonly used for this application, though the results of our analysis apply with minimal modifications to other encryption algorithms when used in the same context. The target GPU architecture for this study is NVidia GeForce GT200 family.

REFERENCES