CryptoGraphics: Secret Key Cryptography Using Graphics Cards

Debra L. Cook
Columbia University
dcook@cs.columbia.edu

John Ioannidis
Columbia University
ji@cs.columbia.edu

Angelos D. Keromytis
Columbia University
angelos@cs.columbia.edu

Jake Luck
10K Interactive
jake301@10k.org

July 16, 2004

Abstract

We investigate the feasibility of using Graphics Processing Units (GPUs) for cryptographic processing by exploiting the ability for GPUs to simultaneously process large quantities of pixels to offload symmetric key encryption from the main processor. We demonstrate the use of GPUs for applying the key stream when using stream ciphers. We investigate the use of GPUs for block ciphers, discuss operations that make certain ciphers unsuitable for use with a GPU, and compare the performance of an OpenGL-based implementation of AES with implementations utilizing general CPUs. We also discuss the applicability of moving encryption and decryption into the GPU to image processing, including the handling of displays in thin-client applications and streaming video, in scenarios in which it is desired to limit exposure of the plaintext to within the GPU on untrusted clients. This avoids temporarily storing the image as plaintext in system memory.

While symmetric key encryption is possible in GPUs, we find that the lack of support via APIs for certain operations results in poor performance overall when using existing ciphers. Furthermore, current APIs do not permit some ciphers to be implemented within the GPU. Our AES experiments prove it is possible to implement AES in a manner that utilizes a GPU to perform the computation while illustrating the difficulty in moving existing block ciphers into the GPU. The lessons learned from developing the OpenGL version of AES indicate GPUs are not suitable, given current APIs, for ciphers involving certain types of byte-level operations. Our work with stream ciphers demonstrates GPUs can be used to offload a shared system CPU in applications which allow large segments of data to be combined with the key stream simultaneously.