ADVANCES IN INFORMATION SECURITY

CryptoGraphics

CryptoGraphics: Exploiting Graphics Cards for Security explores the potential for implementing ciphers within graphics processing units (GPUs), and describes the relevance of GPU-based encryption and decryption to the security of applications involving remote displays.

As a result of the increasing processing power of GPUs, research involving the use of GPUs for general purpose computing has arisen. While GPUs do not support the range of operations found in CPUs, their processing power has grown to exceed that of CPUs and their designs are evolving to increase their programmability. GPUs are especially attractive for applications requiring a large quantity of parallel processing. This work extends such research by considering the use of GPUs as a parallel processor for encrypting data.

The authors evaluate the operations found in symmetric and asymmetric key ciphers to determine if encryption can be programmed in existing GPUs. While certain operations make it impossible to implement some ciphers in a GPU, the operations used in most block ciphers, including AES, can be performed in GPUs. A detailed description and code for a GPU based implementation of AES is provided.

The feasibility of GPU-based encryption allows the authors to explore the use of a GPU as a trusted system component. The motivation for using a GPU as a trusted component, including the applicability to thin-client and remote conferencing applications, is discussed. By enabling encryption and decryption in a GPU, unencrypted display data can be confined to the GPU to avoid exposing it to any malware running on the operating system. A prototype implementation of GPU-based decryption for protecting displays exported to untrusted clients is described. Issues and solutions related to fully securing data on untrusted clients, including the protection of user input, are also discussed.

CryptoGraphics: Exploiting Graphics Cards for Security is designed for a professional audience of researchers and practitioners in industry. This book is also suitable as a secondary text for advanced-level students in computer science.

ISBN 0-387-29015-X

9 780387 290157

springeronline.com ADIS 20

ADIS 20

CRYPTOGRAPHICS
Exploiting Graphics Cards for Security

Cook / Keromytis

ADVANCES IN INFORMATION SECURITY

CryptoGraphics

Exploiting Graphics Cards for Security

Debra Cook
Angelos Keromytis

Springer