WEEK1

Algorithm

30.串联所有单词的子串

https://leetcode-cn.com/problems/substring-with-concatenation-of-all-words/

Review

Reconfiguring the Image Pipeline for Computer Vision

原文知识摘录

A range of vision tasks: object classification, object detection, face identification, optical flow, and structure from motion.

Recent research has focused on dedicated ASICs for deep learning to reduce the cost of forward inference compared to a GPU or CPU.

Image signal processors(ISP) consist of a series of signal processing stages. While the precise makeup of an ISP pipeline varies, we consider a typical set of stages common to all ISP pipelines: denoising, demosaicing, color transformations, gamut mapping, tone mapping, and image compression.

简称

RGB: red, green, blue

CRIP: Configurable & Reversible Imaging Pipeline

ISP: Image signal processor

PSNR: 信噪比

ASIC: 专用集成电路. 目前用CPLD（复杂可编程逻辑器件）和 FPGA（现场可编程逻辑阵列）来进行ASIC设计是最为流行的方式之一

ADC: Analog-to-Digital Converter,指模/数转换器或模拟/数字转换器

CV常用词

propose 提出

depict 描绘

demosaicing 去马赛克

configurable 可配置的

reversible 可逆的

normal distribution 正态分布

uniform distribution 均匀分布

subsample 子样本、二次采样

solid line 实线

dotted line 虚线

asterisk 星号

Usage of botnets for high speed MD5 hash cracking

运用的资源

A. Dictionary Attack

JtR (Jhon the Ripper) is an open source password recovery program, one of whose functions involve dictionary based brute force attacks on hash algorithma including MD5 and SHA.

Distribution of the work of dictionary based attacks to multiple GPUs across networks can be achieved by multiple toolkits like MPI (Message Passing interface).

JtR has been modified by J. R. Crumpacker to be capable of integration with BOINC, an open source middleware system for volunteer grid computing.

B. Brute Force Attack

oclHashCatPlus is a closed source program which utilizes the GPU for performing the brute force attack. It supports various attack modes like mask attack, combinatory attack, dictionary attack, hybrid attack and rule-based attack for a variety of hash algorithms like MD4, MD5, SHA1, NTLM, SHA512, SHA 3 etc. One setback would be the inability to support

remote GPUs for computation.

VirtualCL, a closed source cluster platform that allows OpenCL applications to transparently utilize multiple remote OpenCL devices in a cluster, was used to overcome the inability of oclHashCatPlus to use remote GPUs.

BarsWF is an open source CPU and GPU based MD5 hash cracker. It simultaneously uses the CPU along with the GPU for better hash rates.

Approach

A. Job Calculation and Distribution in Centralized Botnets

Reception of brute force parameters by the C&C servers: Minimum Key length, Maximum Key Length, Character set (Upper case, Lower case, etc.) and hash to be cracked.

1. Reception of brute force parameters by the C&C servers: Minimum Key length, Maximum Key Length, Character set (Upper case, Lower case, etc.) and hash to be cracked.
2. Server's calculation of Job split for each Key Length to available nodes.
3. Distribution of Job Split to each node.
4. Performance of brute force on the given Job Split by simultaneous usage of CPU and GPU (when possible) by each node.
5. Reception of periodic reports of Job processing status by nodes to Server(s).
6. Furnishing of lost Jobs or allocation of Jobs of greater Key Lengths to available nodes.

B. Job Calculation and Distribution in P2P Botnets

C. Node Setup

1. Network module: This module performs all network related operations and is responsible for the botnet's communication as a bot or a combined bot and C&C Server to bots in a private network.
2. Job Splitter module: This performs Job calculation and Distribution as afore described.
3. figuration file editor: This module receives the Job Split information from the overviewing C&C Server through the network module and writes the configuration file from which the Brute Forcing module loads information to perform the brute force attack on the hash.
4. te Forcing module: This performs the brute force attack on the given hash with the configuration specifics contained in the configuration file.

D. Brute Force by Combined Usage of CPU and GPU

简称

C&C server: Command and Control Server

cryptography常用词

mask attack 掩码攻击

combinatory attack 组合攻击

dictionary attack 字典攻击

hybrid attack 混合攻击

rule-based attack 基于规则的攻击

benchmark 基准测试 integration 积分. be capable of integration 具有集成能力

quota 配额

Tip

No zuo no die

这星期没有认真提升技术

Share

https://mp.weixin.qq.com/s/WMlApIA-v8zpB9l-VlMlyw