Using GPUs For OS Kernel Security

Weibin Sun, Robert Ricci
School of Computing, University of Utah
{wbsun, ricci}@cs.utah.edu

Motivation
- Security can be computationally expensive
- dd results on dm-crypt, an encrypted disk, V.S. raw disk:

```
$ wbsun@gpu:~$ sudo dd if=/dev/zero of=/dev/sdb1 oflag=dsync bs=8M count=128
128+0 records in
128+0 records out
1073741824 bytes (1.1 GB) copied, 6.38144 s, 168 MB/s

$ wbsun@gpu:~$ sudo dd if=/dev/zero of=/dev/mapper/b1 oflag=dsync bs=8M count=128
128+0 records in
128+0 records out
1073741824 bytes (1.1 GB) copied, 15.8488 s, 67.7 MB/s
```

- OS Kernel must respond quickly, so time-consuming functionality downgrades system performance
- GPUs are widely deployed and general-purpose enough for OS kernel computation

Challenges(C) & Solutions(S)
- C: GPUs lack hardware features to run a full OS kernel
  S: Offloading only computation intensive code to GPUs, treating GPUs as computing devices.
- C: Data copy to GPU Memory introduces big overhead
  S: Using page-locked memory in CUDA; overlapping copy and execution; high performance APUs will eliminate data copy while providing powerful GPUs
- C: GPU library and driver are not opensource, Linux kernel code can't access them easily
  S: Using a userspace helper to communicate with GPUs for kernel code

System Architecture
- A Linux kernel GPU computing module called KGPU
- Userspace helper to communicate with CUDA runtime
- Concurrent GPU kernels execution and asynchronous data copy

Security Applications
- Encrypted Disk/Filesystem
  - Accelerate eCryptfs, dm-crypt, Cryptloop, CFS, TrueCrypt, ...
- Encrypted Secure Network Connections
  - Accelerate IPSec, SSL, ...
  - Examples of using GPUs for secured network connections: [1],[2].
- Intrusion Detection
  - Accelerate Snort with GPU, e.g. Gnort[3]
- Virus Detection
  - Accelerate virus signature detection, e.g. [4]
- Kernel Module Runtime Verification
  - Too time-consuming on CPU to be integrated into the kernel, GPU may make it more efficient.
  - We are working on GPU-accelerated SMT solver and program analyse.

More(docs, code, news) on Project Website: http://code.google.com/p/kgpu

References
[1] PacketShader: a GPU-accelerated Software Router, Sangjin Han, Keon Jang, KyoungSoo Park and Sue Moon. ACM SIGCOMM 2010
[2] SSLShader: Cheap SSL Acceleration with Commodity Processor, Keon Jang, Sangjin Han, Seungeyop Han, Sue Moon, and KyoungSoo Park. USENIX NSDI 2011

Example-1 eCryptfs
- An encrypted fs in Linux kernel, used by many distributions.
  - 3-4X speedup in Iozone benchmark on NV GTX 480 GPU, Intel X25-M MLC SSD, Intel Core i7 930.
  - Using AES-ECB(as showed)/CTR(similar performance) Ciphers
  - GPU ciphers can support more cipher modes than AES-NI

Example-2 dm-crypt
- Linux encrypted Device Mapper for disk encryption. Kernel part of LUKS.
  - GPU encryption can keep up with an SSD according to the dd benchmark on a similar machine with an Intel X25-E SLC SSD.
  - AES-CTR cipher used.