

ENGSCI YEAR 3 WINTER 2022 NOTES

BRIAN CHEN

Division of Engineering Science

University of Toronto

<https://chenbrian.ca>

brianchen.chen@mail.utoronto.ca

Contents

1	CSC473: Advanced Algorithms	1
1.1	Global Min-Cut	1
2	ECE568 Computer Security	2
2.1	Refresher & Introduction	2
2.1.1	Security Fundamentals	3
3	ECE353 Operating Systems	3
3.1	Kernel Mode	3
3.1.1	ISAs and Permissions	3
3.1.2	ELF (Executable and Linkable Format)	4
3.1.3	Kernel	6

SECTION 1

CSC473: Advanced Algorithms

SUBSECTION 1.1

Global Min-Cut

Given an undirected, unweighted, and connected graph $G = (V, E)$, **return** the smallest set of edges that disconnects G

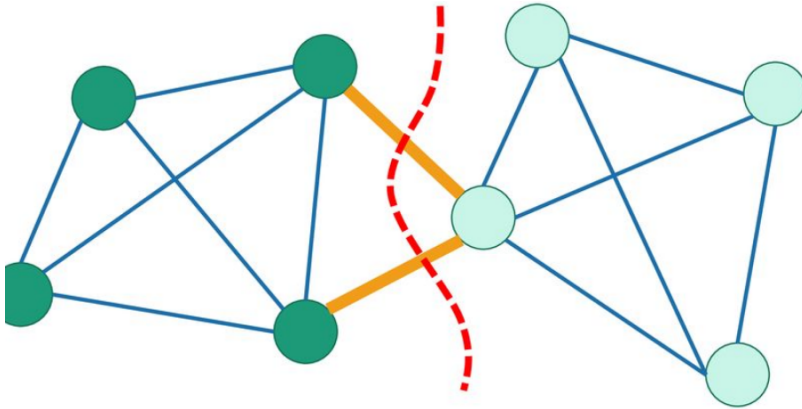


Figure 1. Example of global min-cut. Note that the global min-cut is not necessarily unique

Lemma 1 | If the min cut is of size $\geq k$, then G is k -edge-connected

It may be more convenient to return a set of vertices instead

Definition 1

$$S, T \subseteq V, S \cap T = \emptyset \quad (1.1)$$

$$E(S, T) = \{(u, v) \in E : u \in S, v \in T\} \quad (1.2)$$

The global min-cut is to output $S \subseteq V$ such that $S \neq \emptyset, S \neq V$, such that $E(S, V \setminus S)$ is minimized.

Comment

Note that the min-cut-max-flow problem is somewhat of a dual to the global min-cut problem; the min-cut-max-flow problem imposes a few more constraints than the global min-cut algorithm i.e. having a directed and weighted graph as well as the notion of a source or sink.

- **Input:** Directed, weighted, and connected $G = (V, E)$, $s \in V, t \in V$
- **Output :** S such that $s \in S, t \notin S$ such that $|E(S, V \setminus S)|$ is minimized

We can kind of intuitively see that the global min-cut can be taken to the minimum of all max-flows across the graph. So we can take the max-flow solution and then reduce it to find the global min cut.

Question: how many times will we have to run max-flow to solve the global min-cut problem? Naively, we may fix t to be an arbitrary node, then try every other $s \neq t$ to find the $s - t$ min-cut to get the best global min-cut.

An example of where this may be useful is in computer networks where we can measure the resiliency of a network by how many cuts must be made before a vertex (or many) get disconnected

We know from previous courses that the Edmonds-Karp max-flow algorithm will run in $O(nm^2) = O(n^5)$, which makes our global min-cut algorithm $O(n^6)$. However, there is a paper recently published which gives an algorithm for min-cut in nearly linear time, i.e $O(m^{1-O(1)}) = O(n^2)$ which gives a global min-cut runtime of $O(n^3)$.

A randomized algorithm will be presented that solves this problem in $O(n^2 \log^2 n)$

SECTION 2

ECE568 Computer Security

SUBSECTION 2.1

Refresher & Introduction

Software systems are ubiquitous and critical. Therefore it is important to learn how to protect against malicious actors. This course covers attack vectors and ways to design software securely

Data representation: It's important to recognize that data is just a collection of bits and it is up to us to tell the computer how it should be interpreted. Oftentimes we can make assumptions, for example assume that an int is an int. But what if we end up being wrong about it? Many security exploits rely on data being interpreted in a different way than originally intended. For example,

```

1 unsigned long int h = 0x6f6c6c6548; // ascii for hello
2 unsigned long int w = 431316168567; // ascii for world
3 printf("%s %s", (char*) h, (char*) w);

```

Listing 1: An innocent example of where we should be careful about data representation. This prints hello world

This courses makes use of Intel assembler. TLDR:

- 6 General-purpose registers
- RAX (64b), EAX(32b), AX(16b), AH/AL(8b), etc

Note that the stack grows downwards and the heap grows upwards. Stack overflows can occur and can be a source of vulnerability.

GDB offers some tools for examining stacks

- `break`: create a new breakpoint
- `run`: start a new process
- `where`: list of current stack frames
- `up/down`: move between frames
- `info frame`: display info on current frame
- `info args`: list function arguments
- `info locals`: list local variables
- `print`: display a variable

- `x` display contents of memory
- `fork`: Creates a new child process by duplicating the parent. The child has its own new unique process ID
- `exec`: Replaces the current process with a new process

The fork-exec technique is just a pair of `fork` and `exec` system calls to spawn a new program in a new process

2.1.1 Security Fundamentals

The three key components of security are:

- Confidentiality: the protection of data/resources from exposure, whether it be the content or the knowledge that the resource exists in the first place. Usually via organizational controls (security training), access rules, and cryptography.
- Integrity: Trustworthiness of data (contents, origin). Via monitoring, auditing, and cryptography.
- Availability: Ability to access/use a resource as desired. Can be hard to ensure; uptime, etc...

Together they form an acronym: CIA. A system is considered secure if it has all three of these properties for a given time. The strength of cryptographic systems can be evaluated by the number of bits of entropy or their complexity. For example, a 128-bit key has 2^{128} possible values. This would take a lot of time to break, and a 256-bit key even longer. Availability is hard to measure quantitatively and is instead traditionally measured qualitatively. For example,

SECTION 3

ECE353 Operating Systems

SUBSECTION 3.1

Kernel Mode

3.1.1 ISAs and Permissions

There are a number of ISAs in use today; x86 (amd64), aarch64 (arm64), and risc-v are common ones. For purposes of this course we will study largely arm systems but will touch on the other two as well.

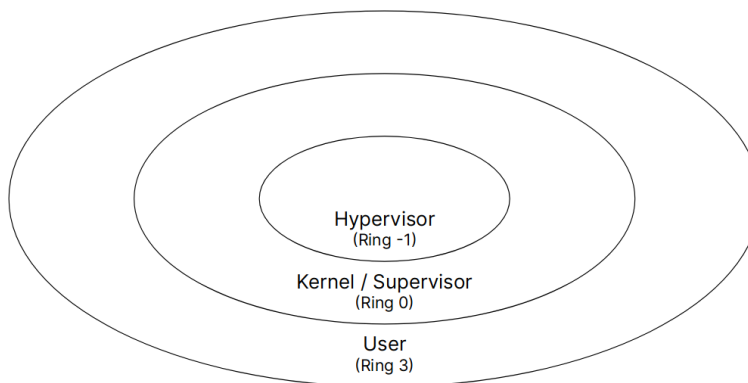


Figure 2. x86 Instruction access rings. Each ring can access instructions in its outer rings.

The kernel runs in, well, Kernel mode. **System calls** offer an interface between user and kernel mode¹.

The system call ABI for x86 is as follows:

Enter the kernel with a `svc` instruction, using registers for arguments:

- `x8` — System call number
- `x0` — 1st argument
- `x1` — 2nd argument
- `x2` — 3rd argument
- `x3` — 4th argument
- `x4` — 5th argument
- `x5` — 6th argument

This ABI has some limitations; i.e. all arguments must be a register in size and so forth, which we generally circumvent by using pointers.

For example, the `write` syscall can look like:

```
1 ssize_t write(int fd, const void* buf, size_t count);
2 // writes bytes to a file descriptor
```

¹Linux has 451 total syscalls

Note: API (application programming interface), ABI (Application Binary Interface). API abstracts communication interface (i.e. two ints), ABI is how to layout data, i.e. calling convention

3.1.2 ELF (Executable and Linkable Format)

- Always starts with 4 bytes: `0x7F`, `'E'`, `'L'`, `'F'`
- Followed by byte for 32 or 64 bit architecture
- Followed by 1 byte for endianness

`readelf` can be used to read ELF file headers.

For example, `readelf -a $(which cat)` produces (output truncated)

Most file formats have different starting signatures or magic numbers

```

1 ELF Header:
2   Magic:   7f 45 4c 46 02 01 01 00 00 00 00 00 00 00 00
3   Class:                                ELF64
4   Data:                                2's complement, little endian
5   Version:                              1 (current)
6   OS/ABI:                                UNIX - System V
7   ABI Version:                           0
8   Type:                                DYN (Position-Independent
    ↳ Executable file)
9   Machine:                              Advanced Micro Devices X86-64
10  Version:                              0x1
11  Entry point address:                   0x32e0
12  Start of program headers:              64 (bytes into file)
13  Start of section headers:             33152 (bytes into file)
14  Flags:                                0x0
15  Size of this header:                   64 (bytes)
16  Size of program headers:              56 (bytes)
17  Number of program headers:             13
18  Size of section headers:              64 (bytes)
19  Number of section headers:             26
20  Section header string table index: 25

```

`strace` can be used to trace systemcalls. For example let's look at the 168-byte hello-world example

This output is followed by information about the program and section headers

```

1 0x7F 0x45 0x4C 0x46 0x02 0x01 0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x00
  ↳ 0x00 0x00
2 0x02 0x00 0xB7 0x00 0x01 0x00 0x00 0x00 0x00 0x78 0x00 0x01 0x00 0x00 0x00
  ↳ 0x00 0x00
3 0x40 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
  ↳ 0x00 0x00
4 0x00 0x00 0x00 0x00 0x40 0x00 0x38 0x00 0x01 0x00 0x40 0x00 0x00 0x00 0x00
  ↳ 0x00 0x00
5 0x01 0x00 0x00 0x00 0x05 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
  ↳ 0x00 0x00
6 0x00 0x00 0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x01 0x00 0x00 0x00 0x00
  ↳ 0x00 0x00
7 0xA8 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0xA8 0x00 0x00 0x00 0x00 0x00
  ↳ 0x00 0x00
8 0x00 0x10 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x08 0x08 0x80 0xD2 0x20 0x00
  ↳ 0x80 0xD2
9 0x81 0x13 0x80 0xD2 0x21 0x00 0xA0 0xF2 0x82 0x01 0x80 0xD2 0x01 0x00 0x00
  ↳ 0x00 0xD4
10 0xC8 0x0B 0x80 0xD2 0x00 0x00 0x80 0xD2 0x01 0x00 0x00 0xD4 0x48 0x65
  ↳ 0x6C 0x6C
11 0x6F 0x20 0x77 0x6F 0x72 0x6C 0x64 0x0A

```

Listing 2: Note: This is for arm cpus

If we run this then we see that the program makes a `write` syscall as well as a `exit_group`

```
1  execve ( " ./ hello_world " , [ " ./ hello_world " ] , 0 x7ffd0489de40
   ↳ /* 46 vars */ ) = 0
2  write (1 , " Hello world \n " , 12) = 12
3  exit_group (0) = ?
4  +++ exited with 0 +++
```

Note that these strings are not null-terminated (null-termination is just a C thing) because we don't want to be unable to write strings with the null character to it.

```
execve("./hello_world_c", ["/./hello_world_c"], 0x7ffbc3444f60 /* 46 vars */) = 0  
brk(NULL)                                = 0x5636ab9ea000  
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3  
fstat(3, {st_mode=S_IFREG|0644, st_size=149337, ...}) = 0  
mmap(NULL, 149337, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7fd4d4384600  
close(3)                                  = 0  
openat(AT_FDCWD, "/usr/lib/libc.so.6", O_RDONLY|O_CLOEXEC) = 3  
read(3, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\3\0\0-\>\0\1\0\0000C"... , 832) = 832  
lseek(3, 792, SEEK_SET)                   = 792  
read(3, "\4\0\0\024\0\0\0\3\0\0\0GNU\0201\336\t\36\251c\324"... , 68) = 68  
fstat(3, {st_mode=S_IFREG|0755, st_size=2136840, ...}) = 0  
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0)  
    = 0x7fd4d4384400  
lseek(3, 792, SEEK_SET)                   = 792  
read(3, "\4\0\0\024\0\0\0\3\0\0\0GNU\0201\336\t\36\251c\324"... , 68) = 68  
lseek(3, 864, SEEK_SET)                   = 864  
read(3, "\4\0\0\024\0\0\0\5\0\0\0GNU\02\0\0\300\4\0\0\3\0\0", 32) = 32
```

Figure 3. A c hello world would load the stdlib before printing...

3.1.3 Kernel

The kernel can be thought of as a long-running program with a ton of library code which executes on-demand. Monolithic kernels run all OS services in kernel mode, but micro kernels run the minimum amount of servers in kernel mode. Syscalls are slow so it can be useful to put things in the kernel space to make it faster. But there are security reasons against putting everything in kernel mode.