Lecture 1 —Introduction, Operating Systems, Security

Jeff Zarnett
jzarnett@uwaterloo.ca

Department of Electrical and Computer Engineering
University of Waterloo

March 4, 2023

Course Syllabus

As our first order of business, let's go over the course syllabus.

Collaborative Course

The source material for the SE 350 notes and slides is open-sourced via Github.

If you find an error in the notes/slides, or have an improvement, go to `https://github.com/jzarnett/se350` and open an issue.

If you know how to use `git` and LaTeX, then you can go to the URL and submit a pull request (changes) for me to look at and incorporate!

Introduction to Operating Systems

Operating systems are those programs that interface the machine with the applications programs. The main function of these systems is to dynamically allocate the shared system resources to the executing programs.

- What Can Be Automated?: The Computer Science and Engineering Research Study, MIT Press, 1980


How likely are you to recommend Windows 10 to a friend or colleague?
1
2
3
4
5
Not at all likely
Extremely likely
Please explain why you gave this score.
I need you to understand that people don't have conversations where they randomly recommend operating systems to one another
THIS IS NOT TRUE
have you ever seen a linux user

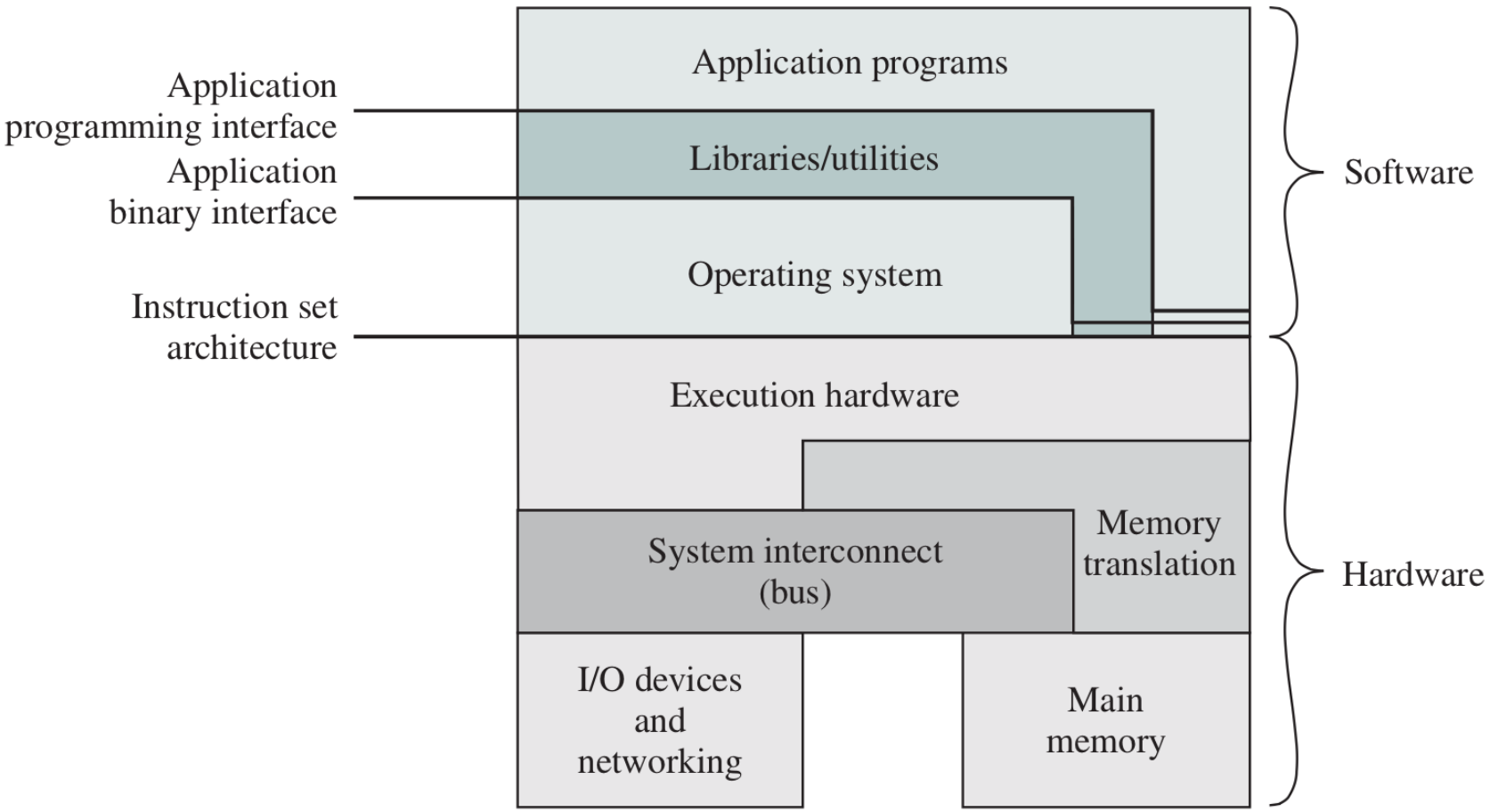
Introduction to Operating Systems

An operating system (OS) sits between the hardware and programs.

It has many goals, that often conflict with one another.

Its job is to make it so other programs can run efficiently.

Structural Diagram of a Modern Computer



OS: Resource Manager

The OS is responsible for resource management and allocation.

Resources like CPU time or memory space are limited.

The OS must decide how to allocate & to keep track of system resources.

In the event of conflicting requests, choose the winner.

OS: Environment Provider

The OS enables useful programs like Photoshop or Microsoft Word to run.

The OS is responsible for abstracting away the details of hardware.

This is so program authors do not have to worry about the specifics.

Imagine Hello World had to be written differently for different hardware.

OS: Multitasking

Multiple programs means some resources are shared.
$\rightarrow$ A source of conflicts!

OS creates and enforces the rules so all can get along.

Sometimes processes want to co-operate and not compete.
The OS can help them to do so.

OS: Efficiency

Another goal may be to use the computer hardware efficiently.

Image Credit: Argonne National Laboratory

Any moment when the supercomputer is not doing useful work is a waste.

OS: What is it, really?

Operating systems tend to be large and do a lot of things.

We expect now that an OS comes with a web browser, an e-mail client, some method for editing text, et cetera.

The part of the operating system we will study is the Kernel.

The kernel is the “core”; the portion of the OS that is always present in main memory and the central part that makes it all work.

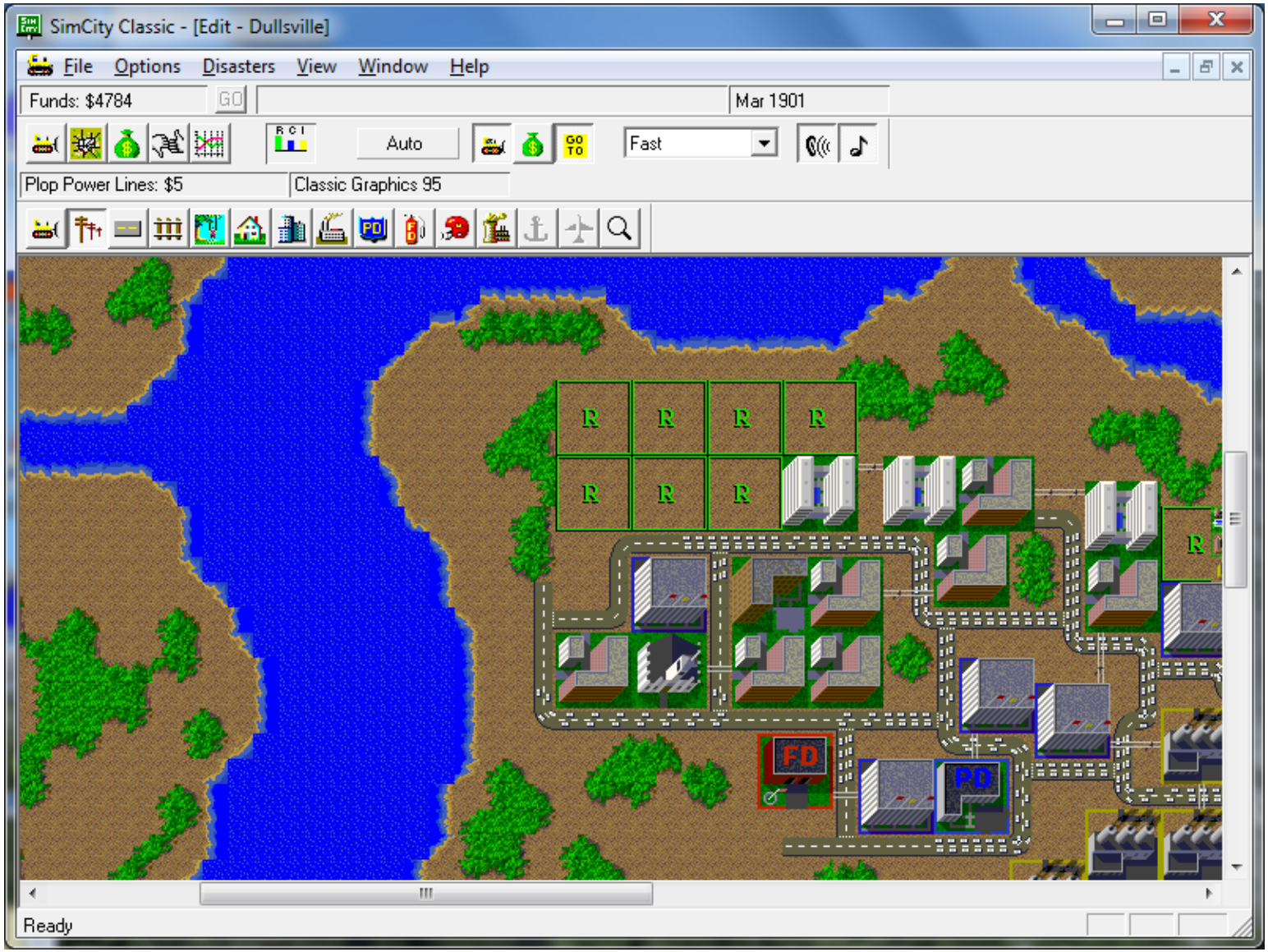
OS: Evolution

Operating systems will evolve over time.

There will be new hardware released, new types of hardware, new services added, and bug fixes.

Evolution is constrained: a need to maintain compatibility for programs.

Example: SimCity and Windows 95



Time, What is Time?

People assume that time is a strict progression from cause to effect, but actually from a non-linear, non-subjective viewpoint, it's more like a big ball of wibbly-wobbly, timey-wimey stuff.

Real-Time vs. Non Real-Time

Real-time systems are the ones where wall-clock deadlines matter.

Examples: aviation, industrial machinery, video conferencing, satellites…

Real-Time Scheduling

There are deadlines, and there are consequences for missing deadlines.

Fast is not as important as predictable.

Hard and Soft Real-Time

Hard real-time: it has a deadline that must be met to prevent an error, prevent some damage to the system, or for the answer to make sense.

If a task is attempting to calculate the position of an incoming missile, a late answer is no good.

A soft real-time task has a deadline that is not, strictly speaking, mandatory; missing the deadline degrades the quality of the response, but it is not useless.

In many textbooks, security and protection are left to the end.

Security has to be designed from the beginning; cannot be bolted on.

An OS supports multiple users with multiple tasks.

Tool Support

OS designers create policies and policy tools.

There is a tradeoff with usability.

You do NOT want to have to report a data breach.

Enforcement is Everything

The OS must enforce the configured policies.
Otherwise, malicious users exploit it.

Three desirable properties: Confidentiality, Integrity, Availability.

Protection vs Security

Protection is about internal threats.

Security is about external threats.

We'll take them in order.

Protection

3rd-level abjuration

Casting Time: 1 action
Range: 30 feet
Components: V, S, M (a miniature silver shield worth 10gp)
Duration: Concentration, up to 1 hour
Class: Bard, Cleric, Druid, Paladin

You trace a warding sigil in the air, sending it to slowly circle a target you can see within range for the next hour. When the target next takes damage, the ward triggers, granting resistance to all damage types except psychic until the end of the target's next turn.

At Higher Levels. When you cast this spell with a spell slot of 4th level or higher, you may target one additional creature for each spell slot level above 3rd.

Art Credit: TES:L

Protection

Most of the discussion in this course is about protection.

Following the rules is important to a functioning system or society.

Even in the absence of malicious intent.

Goals of Protection

Enforce policies about responsible usage.

Responsible and reasonable vary across systems.

Examples of access control: file permissions, walls between processes.

Enforcement is Key

Rules take effort to enforce.

Exceptions are allowed and administrators can override policies!

Other kinds of rules can exist.

Context is Key

If I edit a lecture video, it consumes a lot of CPU and RAM.

Is that bad?

It's legitimate – but might set off alarms.

So we may be lax – which gives an opening to malicious users…

Let's consider a few bad things attackers can do.

Why? We need this in mind when designing the system.

Security Problems

- Breach of Confidentiality
- Breach of Integrity
- Breach of Availability
- Theft of Service
- … and others.

Most likely the weak link is people.

Specific Attacks

A few potential specific attacks:

- **Excessive Requests**
- **Malformed Requests**
- **Back Door**
- **Intercepting Messages**
- **Trojan Horse**

Arms Race

Security is an arms race.

Can we break things if it’s a security problem?

No easy answers.

Security, Conclusion

This is not a course in security, but we can’t ignore it.

Security needs to be included from the beginning!

The Plan

A broad overview of the major topics of the course:

1. Introduction, Security, Review from ECE 252
2. Scheduling
3. Memory
4. I/O Devices, File Systems
5. Reliability, Virtualization/Containers