Software Security

1 Types of memory

Definition: DRAM

1 Transistor per bit

- ”slow”
- cheap

Definition: SRAM

4+ transistors per bit

- fast (~ 4 clock cycles)
- expensive
- Takes up space on die

2 Computer Architecture

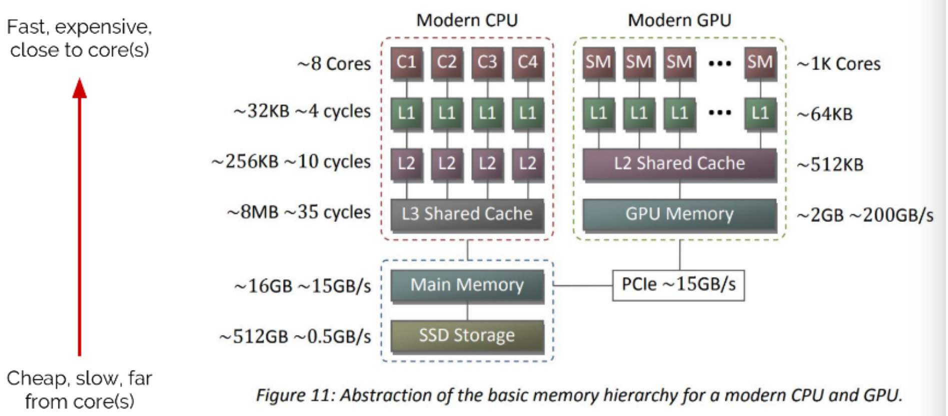
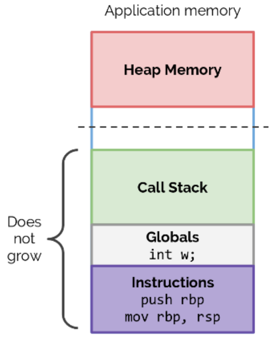


Figure 11: Abstraction of the basic memory hierarchy for a modern CPU and GPU.

3 GPU

GDDR5 is ”slow” and cheap

4 The Stack

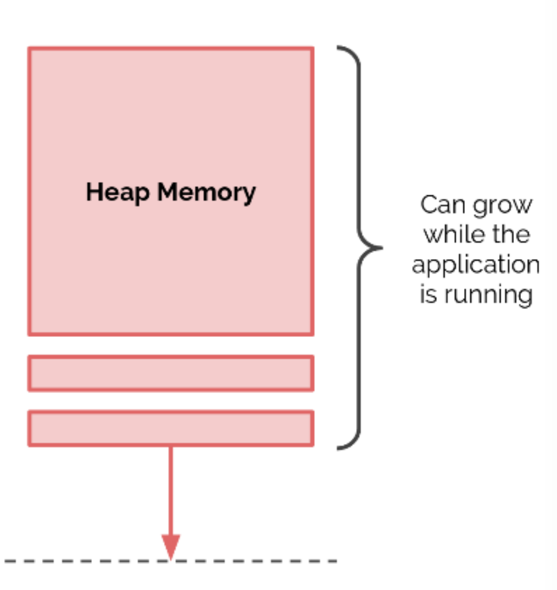


- When a program thread starts, the operating system reserves some amount of space for the stack - stack memory does not grow during runtime

The stack being full is cased by

- Badly written recursive functions
- Too much local memory allocated (especially with multi-threading)

5 The Heap



- Memory is not guaranteed to be initialised to zero
- Can malloc memory to same size of some sensitive data

6 Understanding the platform

- The key to writing good, secure software is to understand the platform
- Hardware is the base platform (for software)
- Lots of things get in the way