Software Security
COSC 466/566
Spring 2023

Dr. Doowon Kim

THE UNIVERSITY OF
TENNESSEE

Today’s class

- Introducing
- Security mindset
- What’s the computer security?

Who are you? (Trying to remember your name)

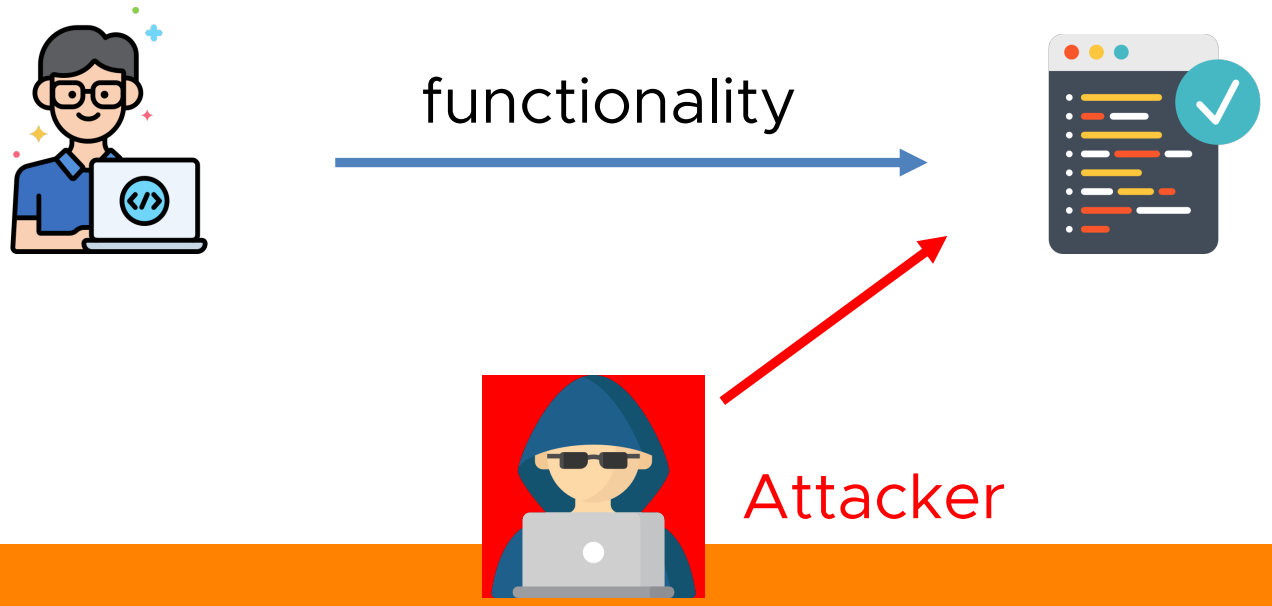
- Preferred name
- Class year
- Academic program and advisor if possible
- Background in Security (a lot, a little, none)
- What do you expect to learn from this course?
- What topic interests you the most?
- Why do you choose this course?

THE UNIVERSITY OF TENNESSEE KNOXVILLE

What is computer security?

The key difference:

- Security involves an adversary who is active and malicious.
- Attackers seek to circumvent protective measures.



THE UNIVERSITY OF TENNESSEE KNOXVILLE

What's the diff between you and attackers?

- Attackers are not normal users

- Normal users: try to avoid bugs/flaws
- Attackers: try to find the bugs/flaws out and to exploit them

THE UNIVERSITY OF TENNESSEE KNOXVILLE

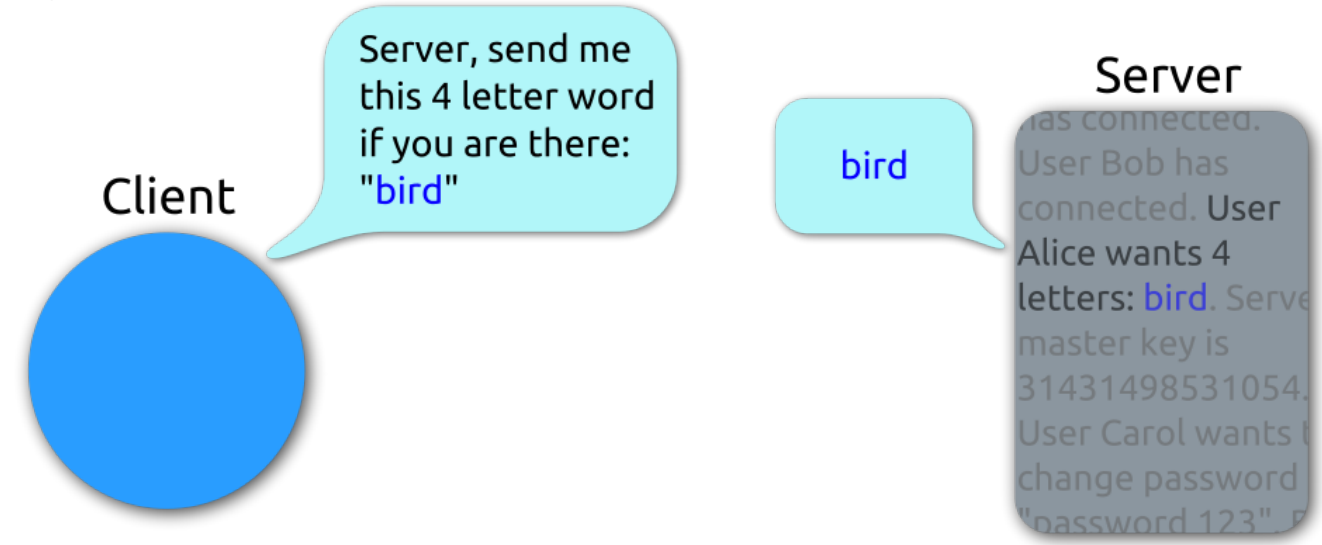
Ex) The Heartbleed Bug

- A security bug in the OpenSSL cryptography library, which is widely used implementation of the Transport Layer Security (TLS) protocol **[wikipedia]**
  - This weakness allows stealing the information
    - user names & passwards
    - instant messgaes & emails
    - business critical documents & communication
    - more..

Ex) The Heartbleed Bug

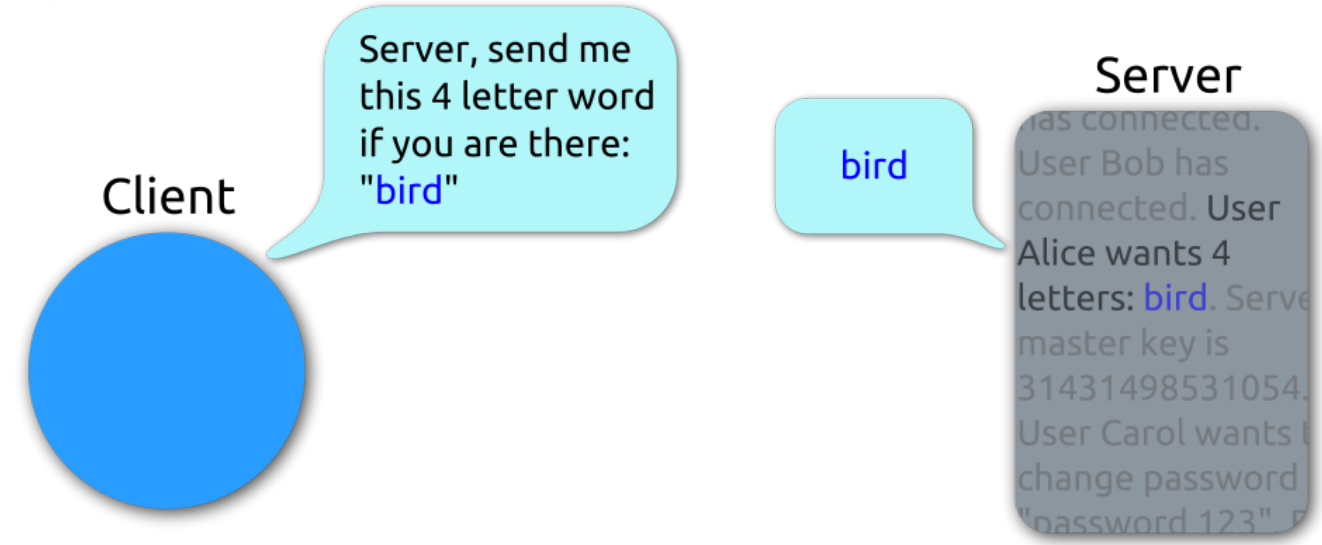
- The vulnerability is a “buffer over-read”
  - Software (accidently) allows more data to be read than should be allowed

Heartbeat – Normal usage

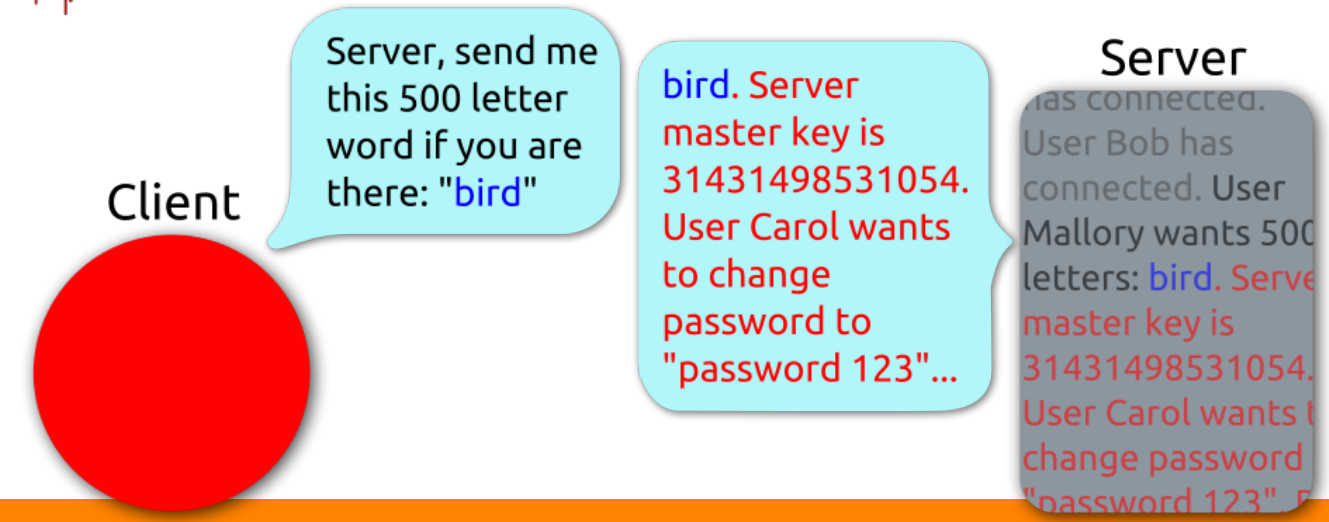


THE UNIVERSITY OF TENNESSEE KNOXVILLE

Heartbeat – Normal usage



Heartbeat – Malicious usage



THE UNIVERSITY OF TENNESSEE KNOXVILLE

Ex) The Heartbleed Bug

- The vulnerability is a “buffer over-read”
  - Software (accidently) allows more data to be read than should be allowed
- It is a simple programming bug, but it is hard to discover
  - Vulnerable OpenSSL was released on March 14, 2012
  - Google’s security team reported Heartbleed on April 1, 2014

How to find a problem?

- Manual program inspection
  - Maybe effective
  - But humans are not good at
    - Repetitive and tedious tasks
    - Maintaining large amounts of detail
- Automated program analysis
  - Replace human inspection to find software problems
  - Support inspection by
    - Automated extracting and summarizing information
    - Automatically analyze extracted information

Capture The Flag (CTF)

https://en.wikipedia.org/wiki/Capture_the_flag

THE UNIVERSITY OF TENNESSEE KNOXVILLE

What’s the CTF?

- Capture the Flag (CTF) in computer security is an exercise in which "flags" are secretly hidden in purposefully-vulnerable programs or websites.

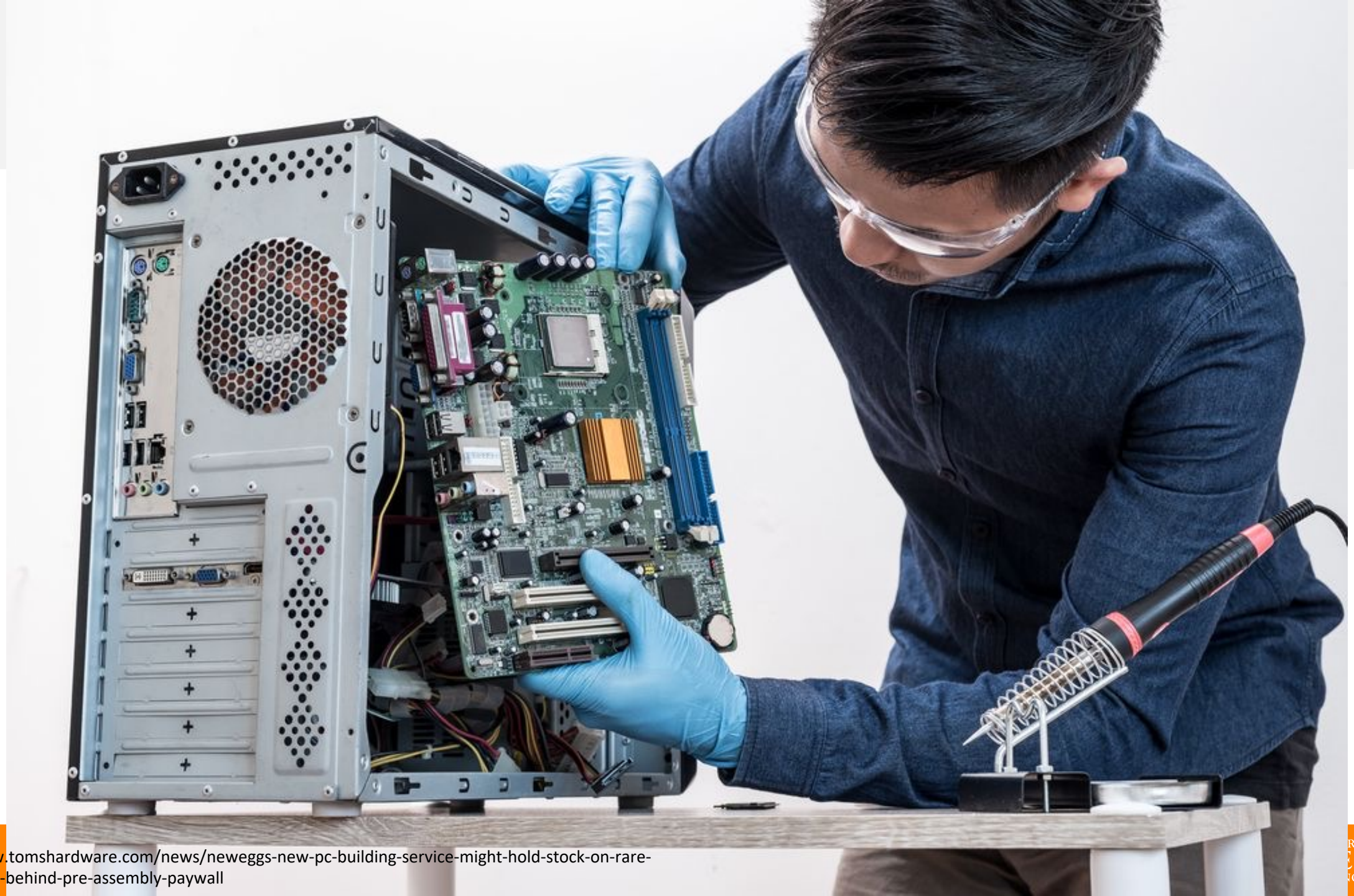
Demo

- SignUp Bonus

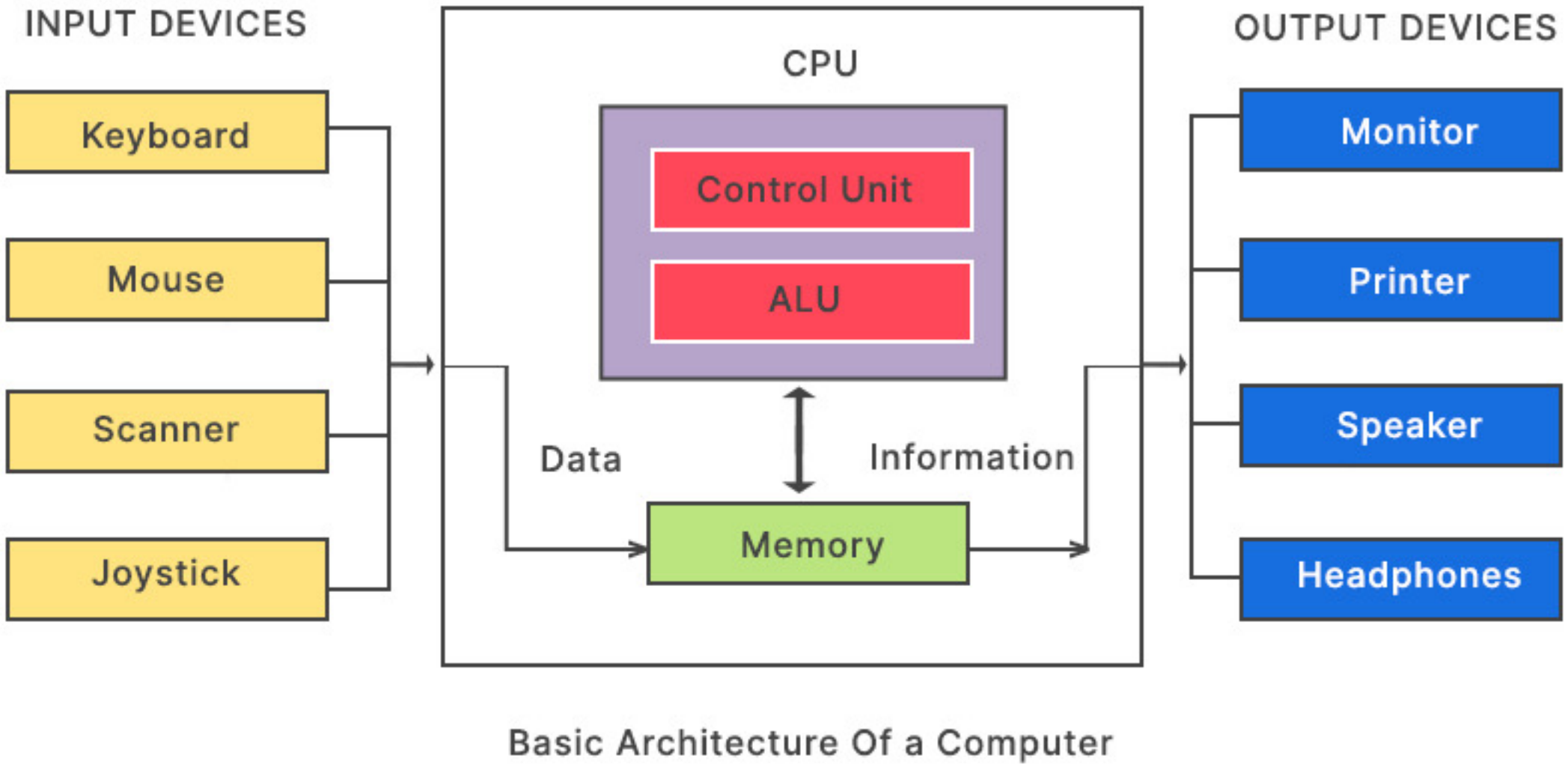
Demo

- Play with images

Machine Programming: Basics



https://www.tomshardware.com/news/neweggs-new-pc-building-service-might-hold-stock-on-rare-components-behind-pre-assembly-paywall



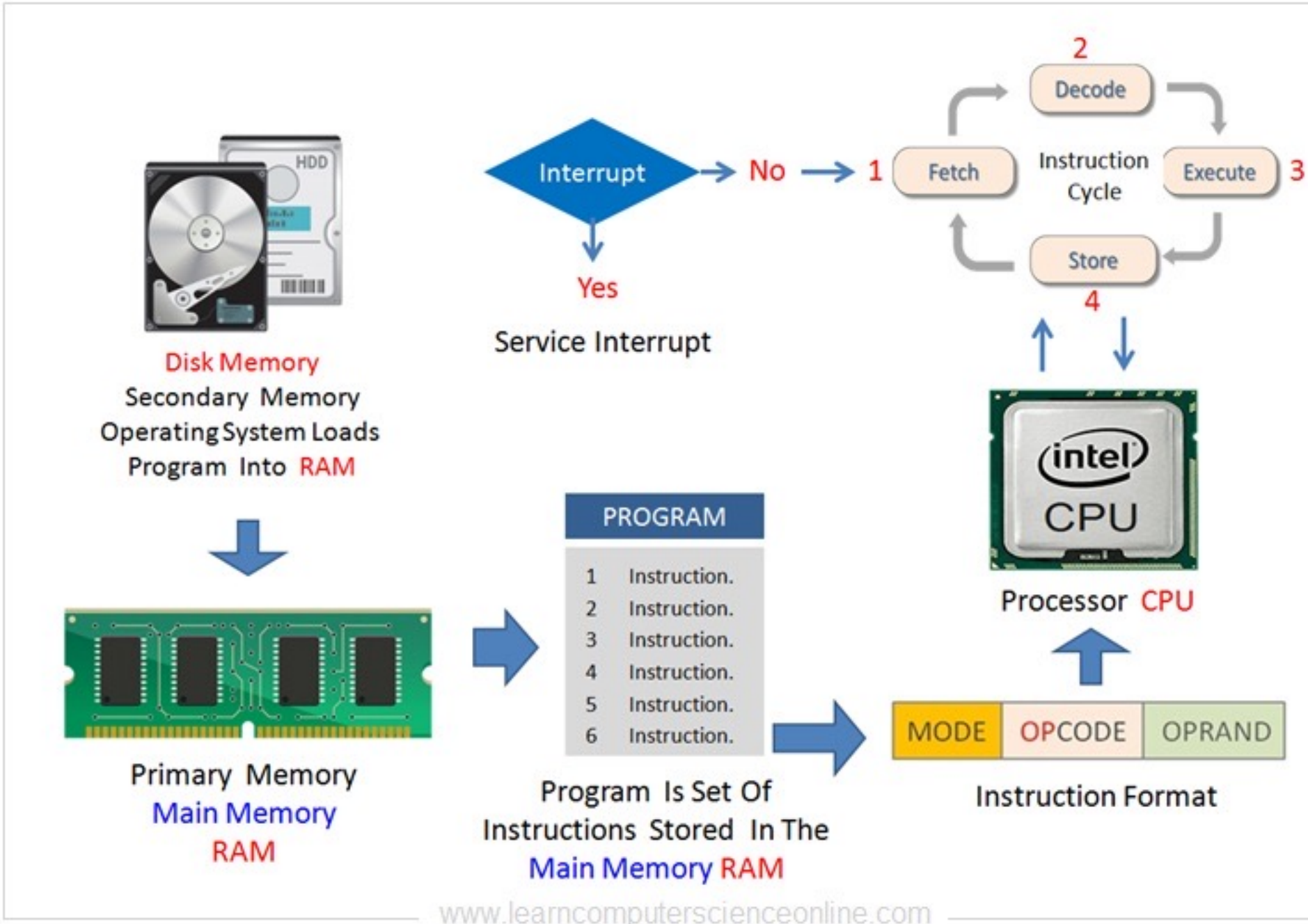
Basic Architecture Of a Computer

https://www.google.com/url?sa=i&url=https%3A%2F%2Funstop.com%2Fblog%2Fdifference-between-computer-architecture-and-computer-organization&psig=AOvVaw1Wty1rKROf5WOoCGSCeqrz&ust=1675126038977000&source=images&cd=vfe&ved=0CBAQjhxqFwoTCODc9_WI7vwCFQAAAAAdAAAAABBO

Central Processing Unit (CPU)

- Provides computation
  - The set of allowed operations is known as the instruction set
  - Machine code is the byte-level programs that the processor executes
  - Assembly code is a human-readable representation of machine code
- Provides limited storage
  - Registers
  - Cache
- Interfaces with rest of computer
  - PCI
  - Main memory
  - USB

THE UNIVERSITY OF TENNESSEE KNOXVILLE



www.learncomputerscienceonline.com

UNIVERSITY OF TENNESSEE KNOXVILLE

CPU Architectures

- Instruction set
  - Reduced instruction set computer (RISC)
    - General operations
    - Power efficient
    - Example: ARM
  - Complex instruction set computer (CISC)
    - Complex and specialized operations
    - Pipelining allows for incredible throughput
      - Modern side-channel attacks take advantage of these complex pipelines
    - Example: Intel Core i7, AMD Ryzen
- Architecture also specifies the word size
  - Refers to the default numbers of bits for data and pointers
  - Modern systems use 64-bit (8-bytes) words

THE UNIVERSITY OF TENNESSEE KNOXVILLE

x86 Chipsets

- Intel released several backwards compatible chips
  - 80186, 80286, 80386, i486 (80486)
  - Shared instruction set known as x86
- Intel Pentium processors
  - Next evolution of the x86 architecture
  - Higher clock speeds, more pipelining
  - Pentium 4E was the first 64-bit consumer-grade CPU
- AMD Athlon processors
  - Used machine code that was compatible with intel
  - Cemented x86 as the dominant instruction set

THE UNIVERSITY OF TENNESSEE KNOXVILLE

x86 Chipsets

- Core processors
  - Transitioned from focusing on increasing clock frequency to increasing core counts
    - Marginal gains by increasing clock speed
    - More power efficient
  - Based on the Pentium 3 architecture
  - 64-bit architecture
- AMD continued to produce chips compatible with Intel's chips
  - Usually, less performant
  - Much cheaper

THE UNIVERSITY OF TENNESSEE KNOXVILLE

Moving to 64-bit Architectures

- IA-64
  - Intel's attempt to create a new instruction set for 64-bit processors
  - Was not backwards compatible with the x86 instruction set
  - Was a failure
- x86-64
  - AMD's proposed 64-bit instruction set
  - Was backwards compatible with the x86 instruction set
  - Currently used by Intel and AMD processors

THE UNIVERSITY OF TENNESSEE KNOXVILLE