Technologies: Linux, Virtual Machines, Cloud Computing and Containers

Introduction to Computer Security

Naercio Magaia and Imran Khan

Contents

- Linux
- Command Line Interfaces
- Apache Web Server
- Virtual Machines
- Amazon Web Services
- Containers and Docker

What is Linux?

- Linux is a clone of Unix
  - Unix was one of the first multitasking and multiuser operating systems from Bell Labs in 1969
- Open-Source operating system providing full multitasking across multiple architectures
- Created in 1991 by Linus Torvald and supported by a very large community
- It is free, unlike Windows, MacOs, and iOS (Android offshoot of Linux)

What is Linux?

- Available in a wide variety of distributions
  - A distribution is a chosen Linux kernel, a package management system and a set of applications
  - Some are commercially backed: RedHat, openSUSE
  - Others community managed: Debian, Gentoo…
  - We'll be using Ubuntu, commercially managed by Canonical Ltd, based on Debian and very stable

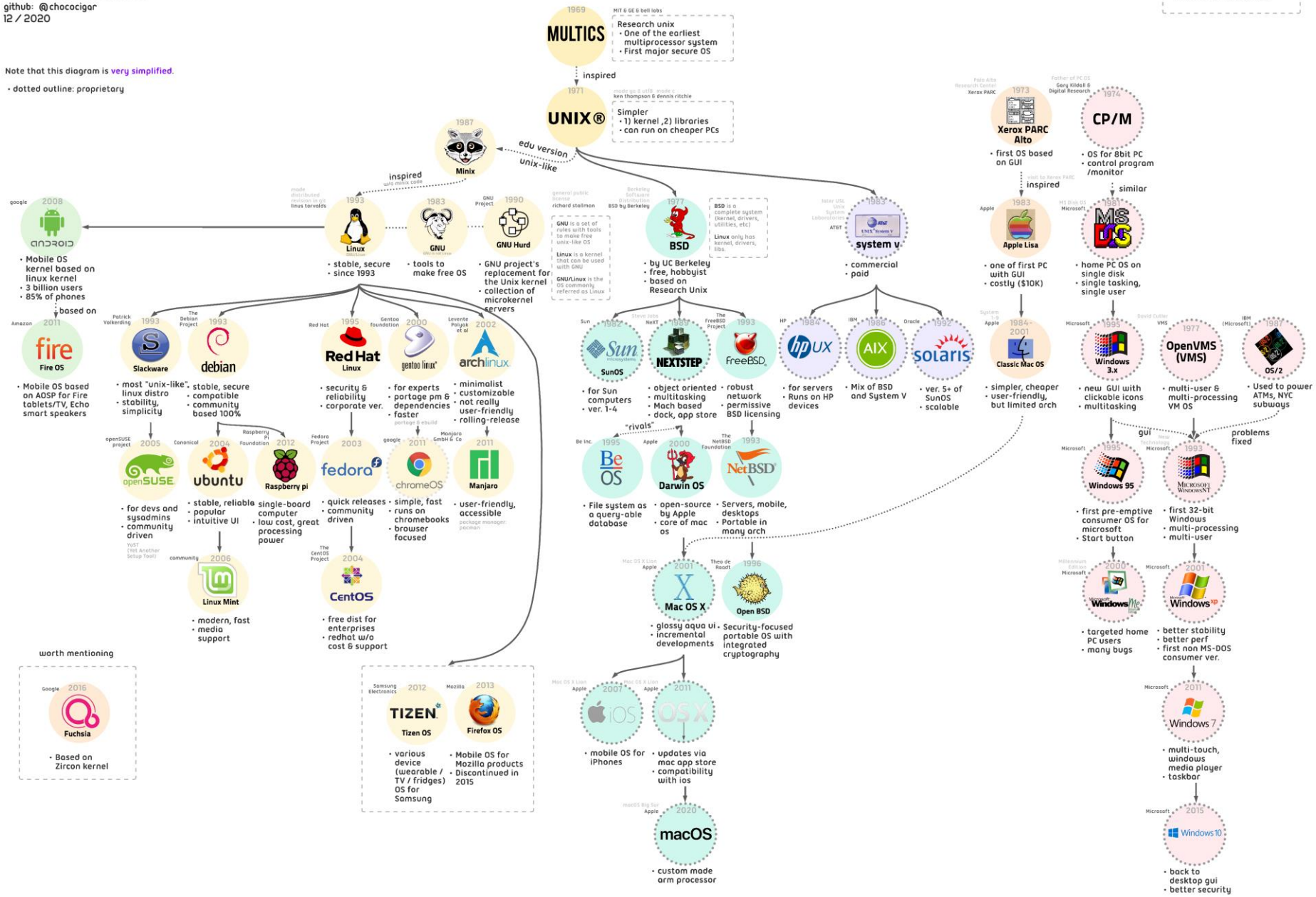
SIMPLE HISTORY OF OS

for any corrections, please contact
github: @chococigar
12 / 2020

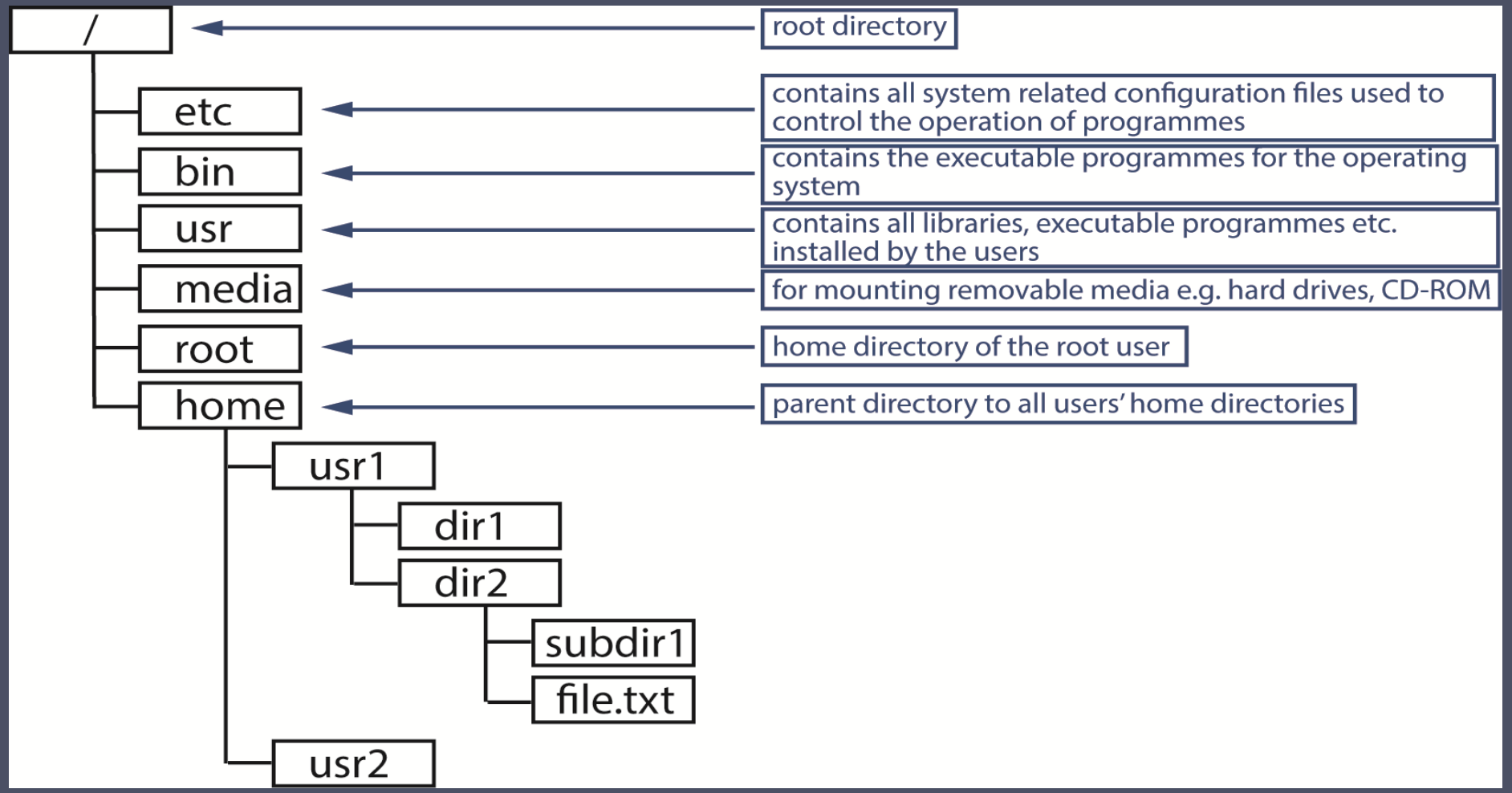
Note that this diagram is very simplified.

- dotted outline: proprietary

POSIX (Portable Operating System Interface)
- IEEE standard for maintaining compatibility between OS's
- most unix-like systems



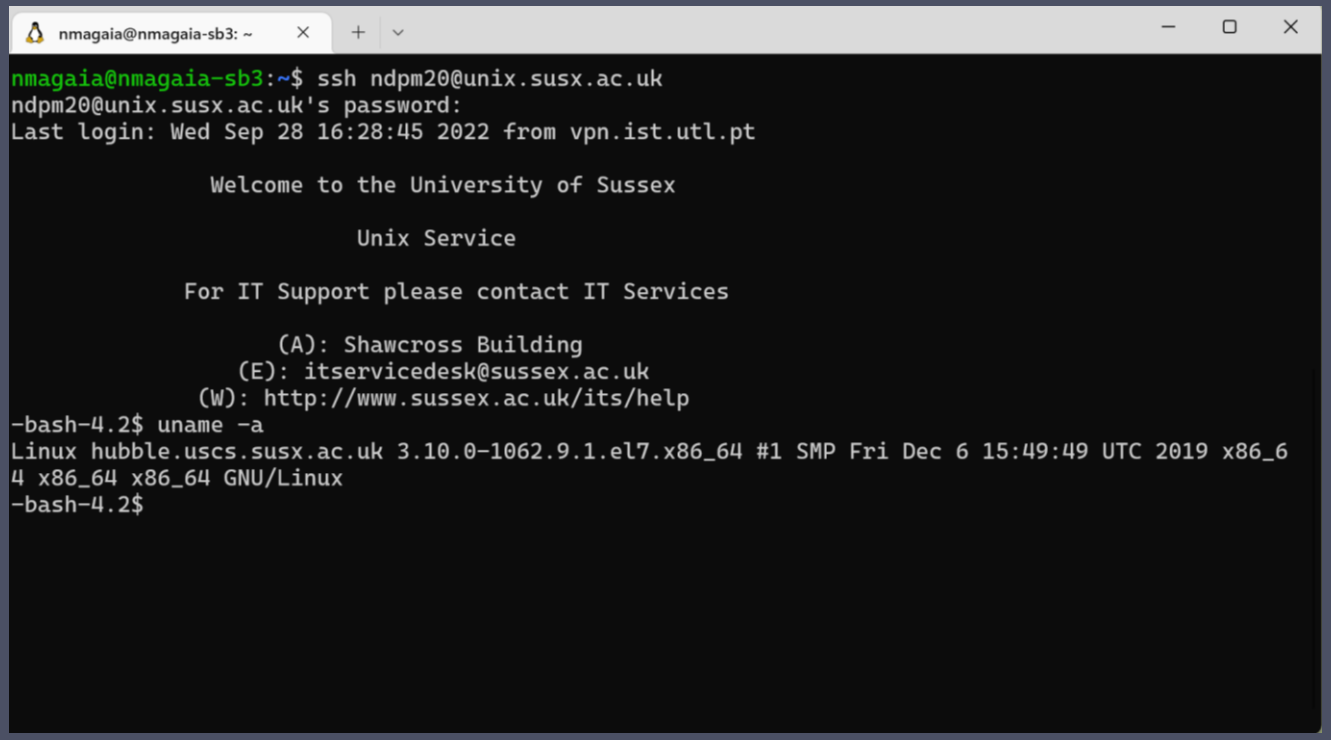
Linux File System



- Hierarchical directories (folders), starting at root
- Standardised locations
- Easily explored from the Command Line Interface (CLI)

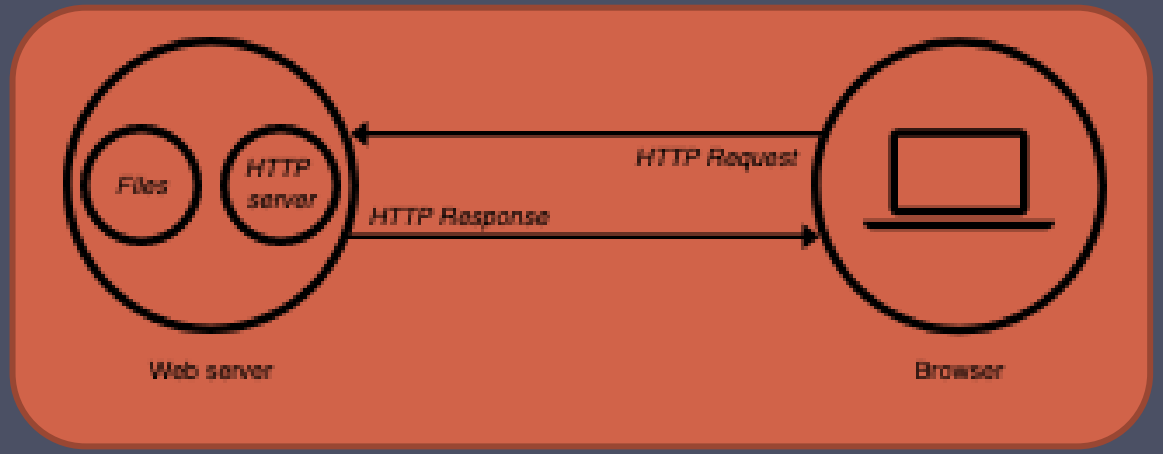
Command Line Interface

- All human computer interfaces can be a way to interact with the “shell” around the application and operating system
- Most operating systems have a command line interface that provides a set of commands to interact directly with the operating system
- Have a play on the Sussex Unix server



Apache HTTP Server

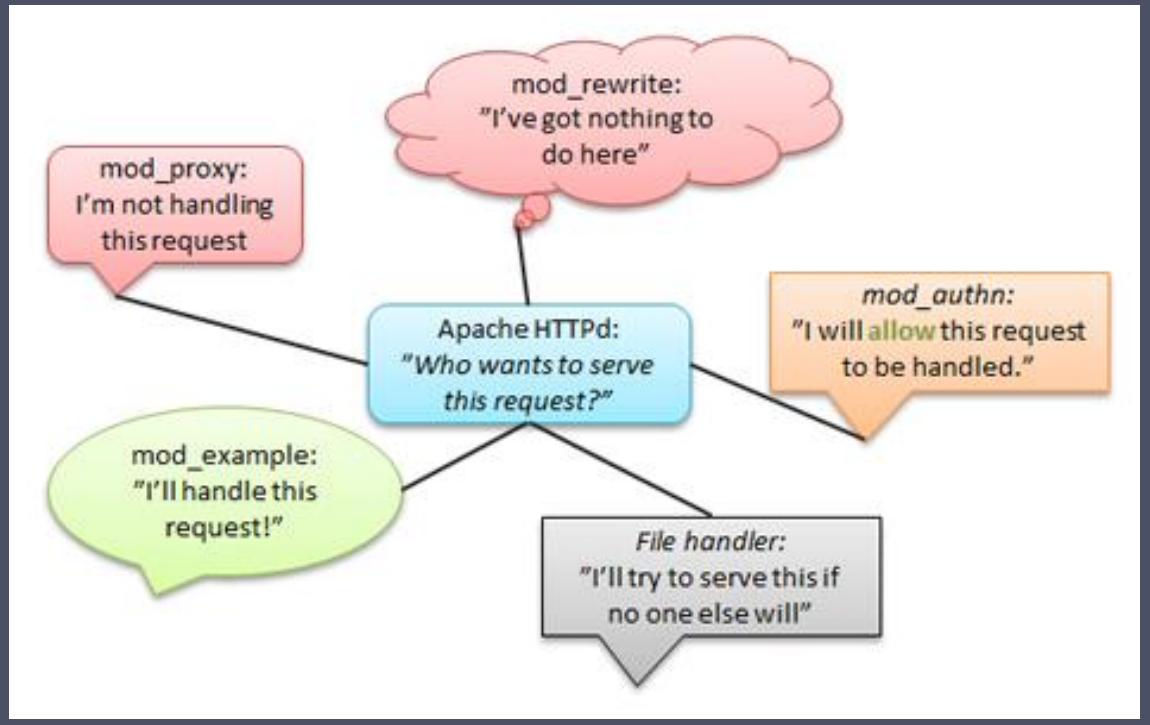
- Web servers listen on a TCP port for HTTP requests
- They process the request, then return a response on the same TCP connection
- Apache is open source and runs well over a quarter of the Web



- Easy to install and configure on Linux
- Available in packages for your computer, e.g., XAMPP and WAMP

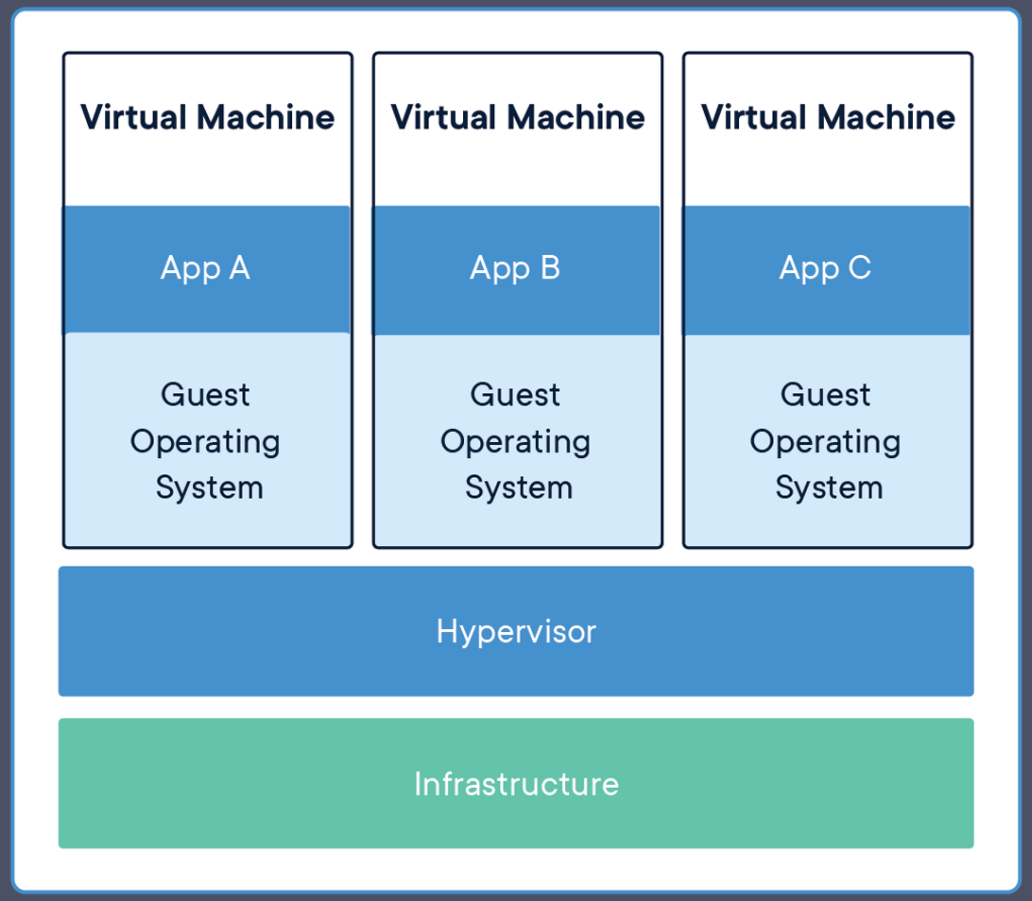
Apache functionality

- `/etc/httpd/conf/httpd.conf`
  - Directives such as:
  - `DocumentRoot` (Where the content is)
  - `Listen` (what port, e.g., 80 or 8080)
  - `LogLevel` (how much to log)
- Allows for native interpreters via modules for PHP, Python, Ruby and Perl
- Other modules for authorization, rewrites, etc.
- Place HTML and other files in directories under the DocumentRoot to provide access



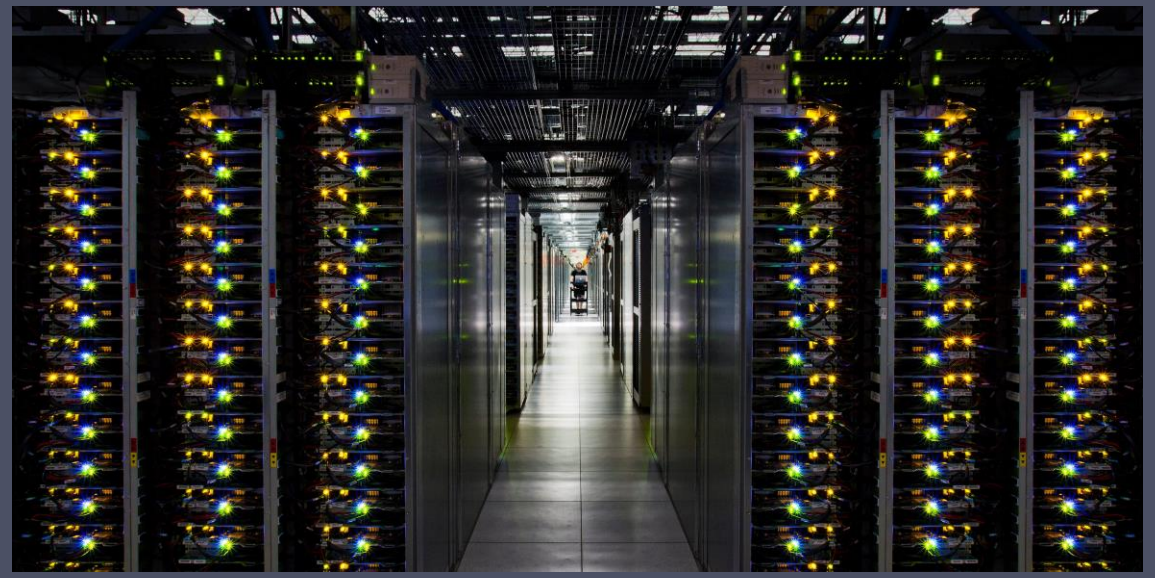
Virtual Machines

- An operating system abstracts the hardware so multiple processes can run
- Machine virtualization is an **abstraction of hardware** so that multiple operating systems can run concurrently
- A hypervisor provides the **interface abstractions** for this to happen
- A **full copy** of the OS is installed on every VM
- Commonly used by cloud providers to deliver multiple instances on a single server



Cloud Computing

- Most computing takes place in Data Centres
- Servers and Storage Systems are connected by local area networks with egress and ingress to the wider Internet
- Commercial providers leverage their Data Centres to provide cloud service, notably Microsoft Azure, Google and Amazon Web Services

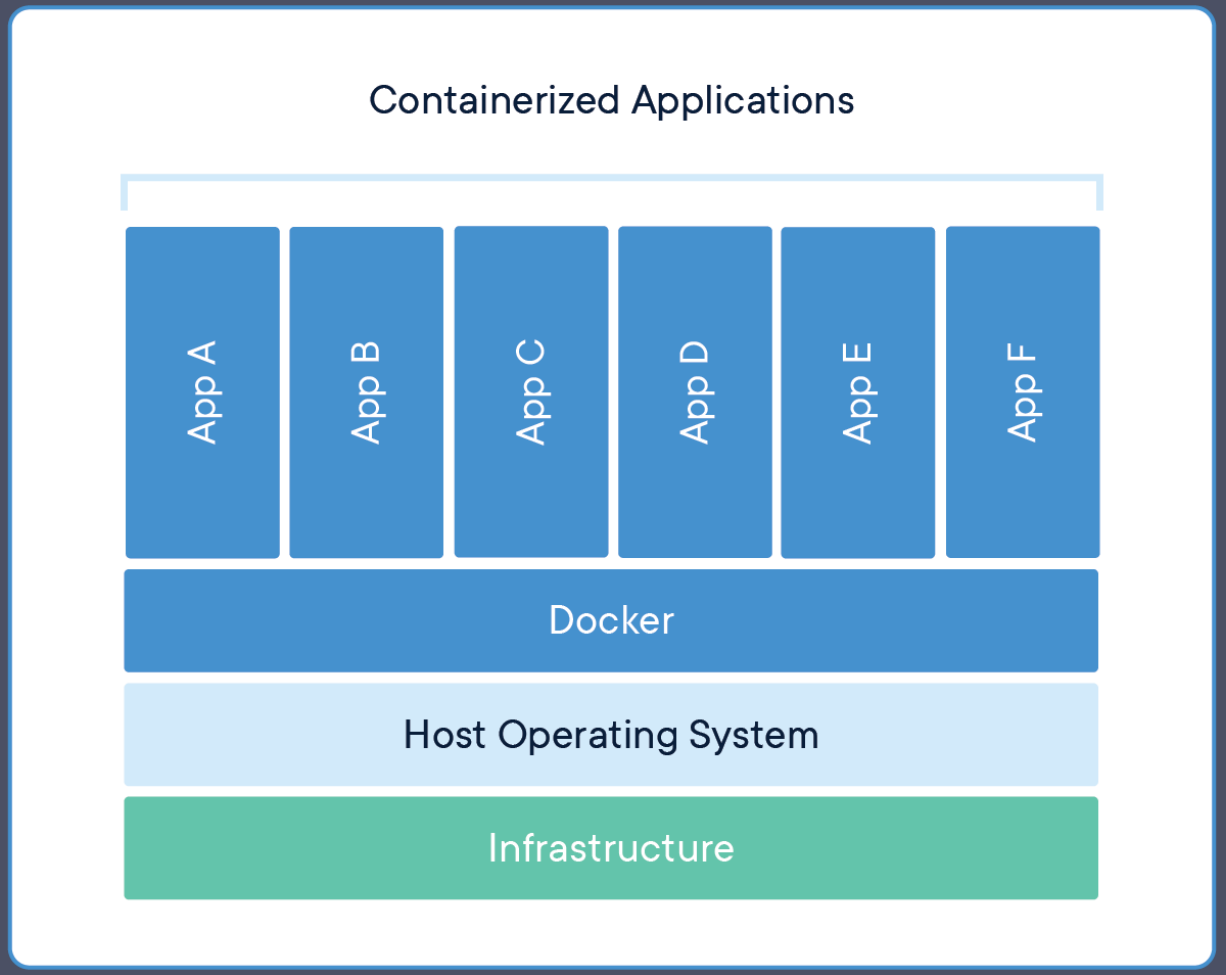


Amazon Web Services

- Provides a rich set of services and technologies located in Amazon's Data Centres
- Provides very low-cost entry to computing on demand
- Applications are built from databases, other services and the set of Web servers and load balancers that provide access
- Well designed Web interface to manage services, such as instances (Elastic Compute 2 (EC2)), and locate in a centre around the world
- https://aws.amazon.com/ec2/getting-started/

Containers

- Rather than packaging the whole OS, software can provide namespace management within a Process to isolate applications (rebasing the apps view of the directory structure, and catching and redirecting the signals)
- Applications can be packaged with the other applications and services needed and run in a user space process
- Docker is the most well known



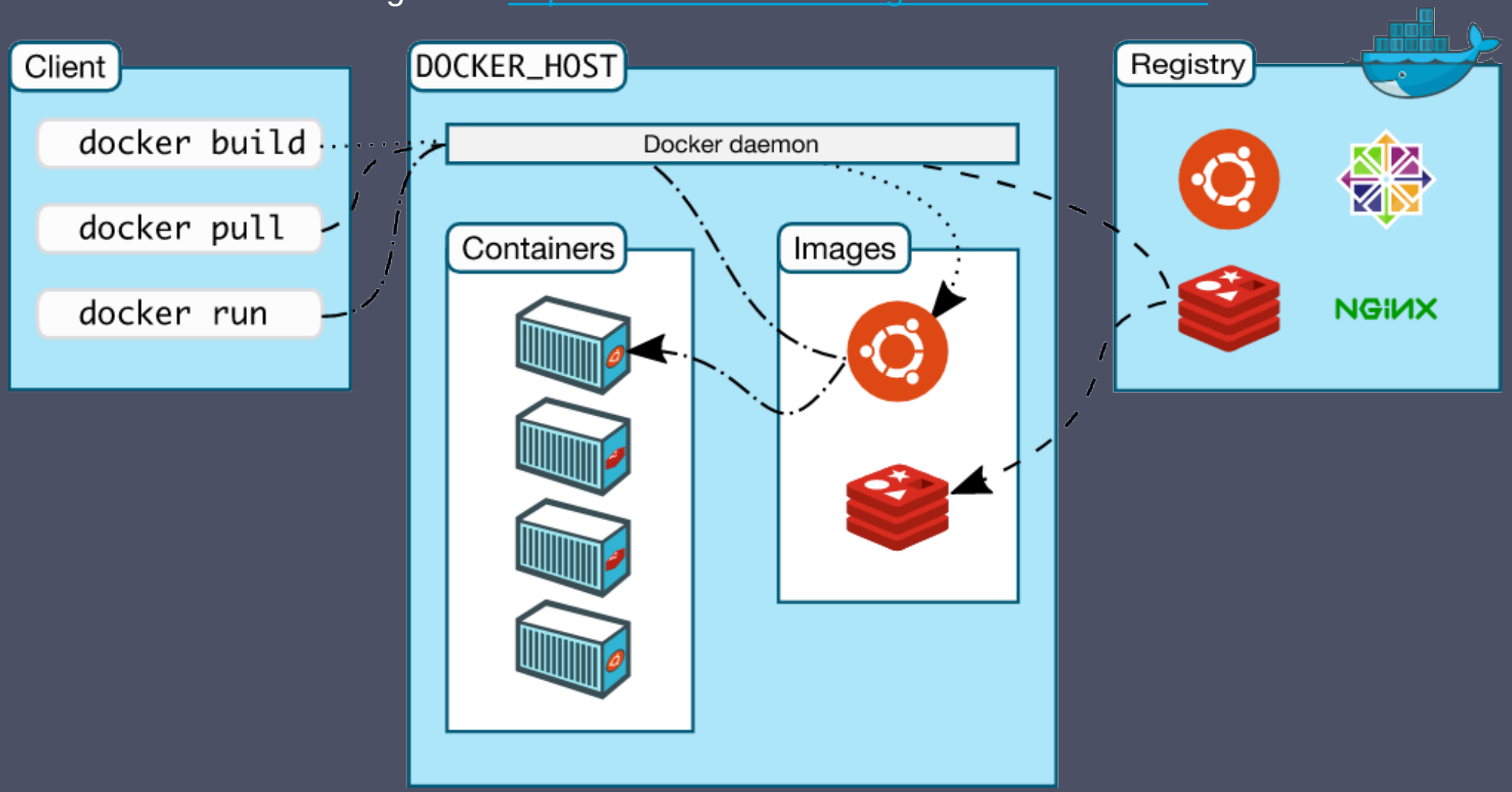
Docker

- A Docker container image is a lightweight, standalone, executable package of software that includes everything needed to run an application: code, runtime, system tools, system libraries and settings.
- An image becomes a container when it runs on a container runtime, e.g., Docker Engine

- *Image* is built and stored on a *registry*
- The container Daemon runs on the target machine
- The Daemon pulls images from the registry
- Starts a process that turns the image into a container
- The container maps onto the standard input and output of the target
- Network sockets can create virtual networks, or even map through to real interfaces

Docker Flow

Original at https://docs.docker.com/get-started/overview/



Docker and this Module

- We want to probe applications such as databases and web servers
  - Putting vulnerable software on your machine is not recommended
- Docker provides isolated instance of the applications running on your computer, which go up and down as you control through Docker.
- Docker and other container technologies are widely used to test and distribute applications
- https://docs.docker.com/get-started/

Conclusion

- Technologies in use on this course:
  - Linux and the CLI
  - Cloud Computing Services and AWS
  - Containers and virtual machines
  - Docker
- Have a play with the Command Line Interface on the Sussex Unix server