FIT 1047

Introduction to computer systems, networks and security

Overview

- PC boot sequence
- BIOS / UEFI

Booting a PC

How to load the operating system?

- requires drivers (software!)

Booting a PC

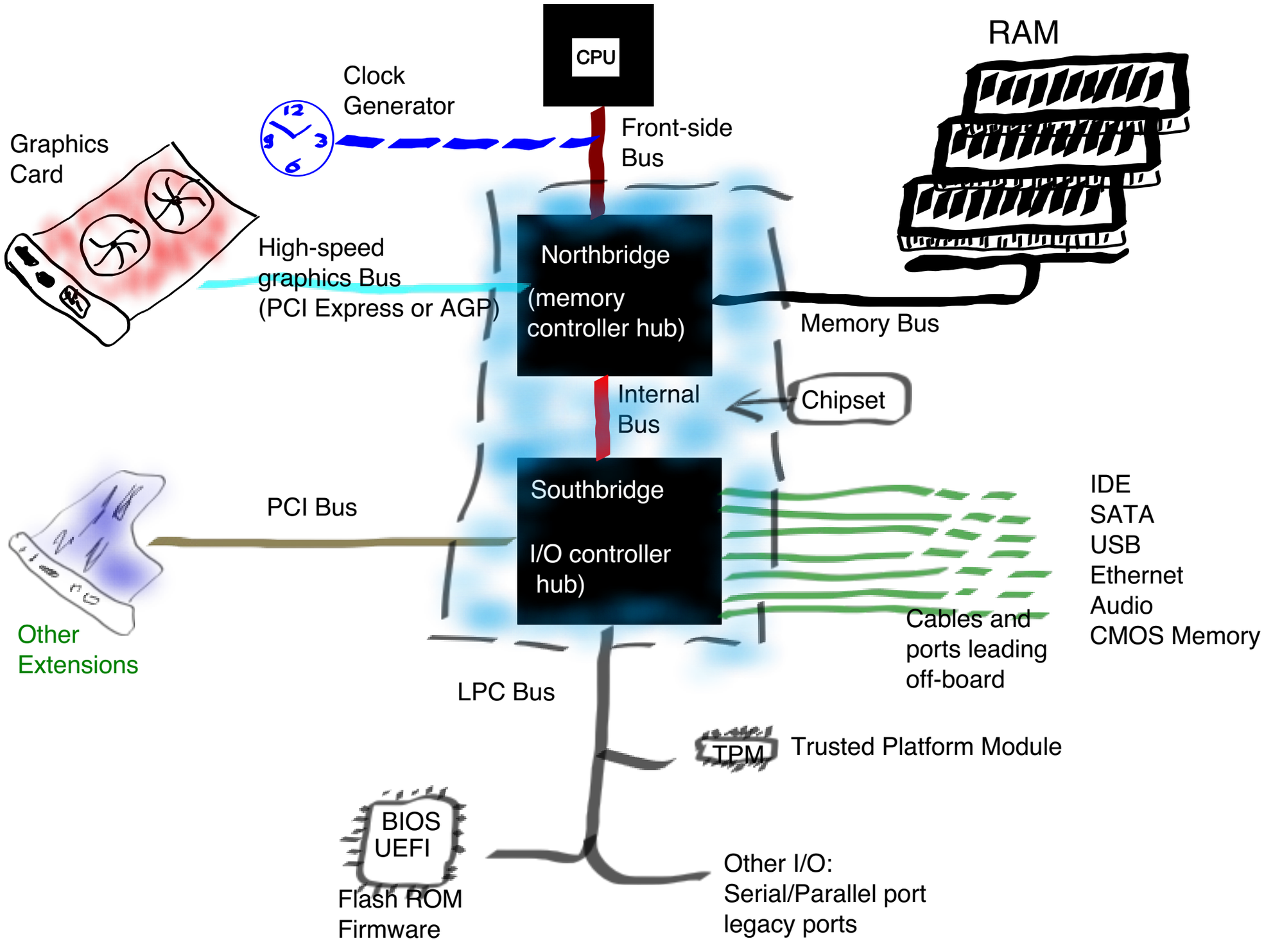
How to load the operating system?

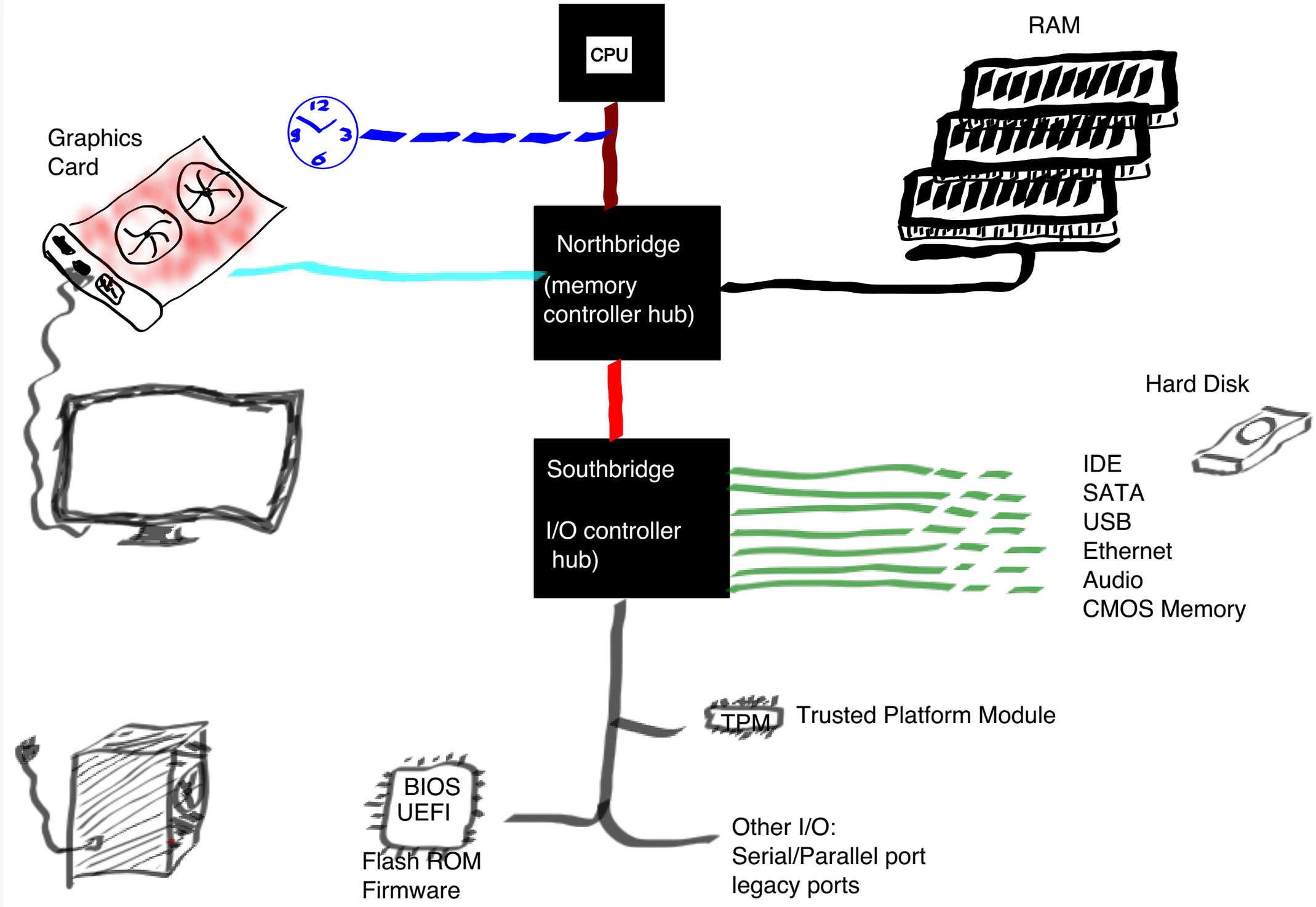
- requires drivers (software!)

Who loads the drivers?

Booting a PC

Pull oneself up by one's bootstraps


CPU
RAM
Clock
Generator
Front-side
Bus
Graphics
Card
High-speed
graphics Bus
(PCI Express or AGP)
Northbridge
(memory
controller hub)
Memory Bus
Internal
Bus
Chipset
Southbridge
I/O controller
hub)
PCI Bus
IDE
SATA
USB
Ethernet
Audio
CMOS Memory
Cables and
ports leading
off-board
Other
Extensions
LPC Bus
TPM
Trusted Platform Module
BIOS
UEFI
Flash ROM
Firmware
Other I/O:
Serial/Parallel port
legacy ports


CPU
RAM
Graphics Card
Northbridge
(memory controller hub)
Hard Disk
Southbridge
I/O controller hub)
IDE
SATA
USB
Ethernet
Audio
CMOS Memory
TPM
Trusted Platform Module
BIOS
UEFI
Flash ROM
Firmware
Other I/O:
Serial/Parallel port
legacy ports

Boot process

Boot process

- Turn power on

Boot process

- Turn power on
- Power good?

Boot process

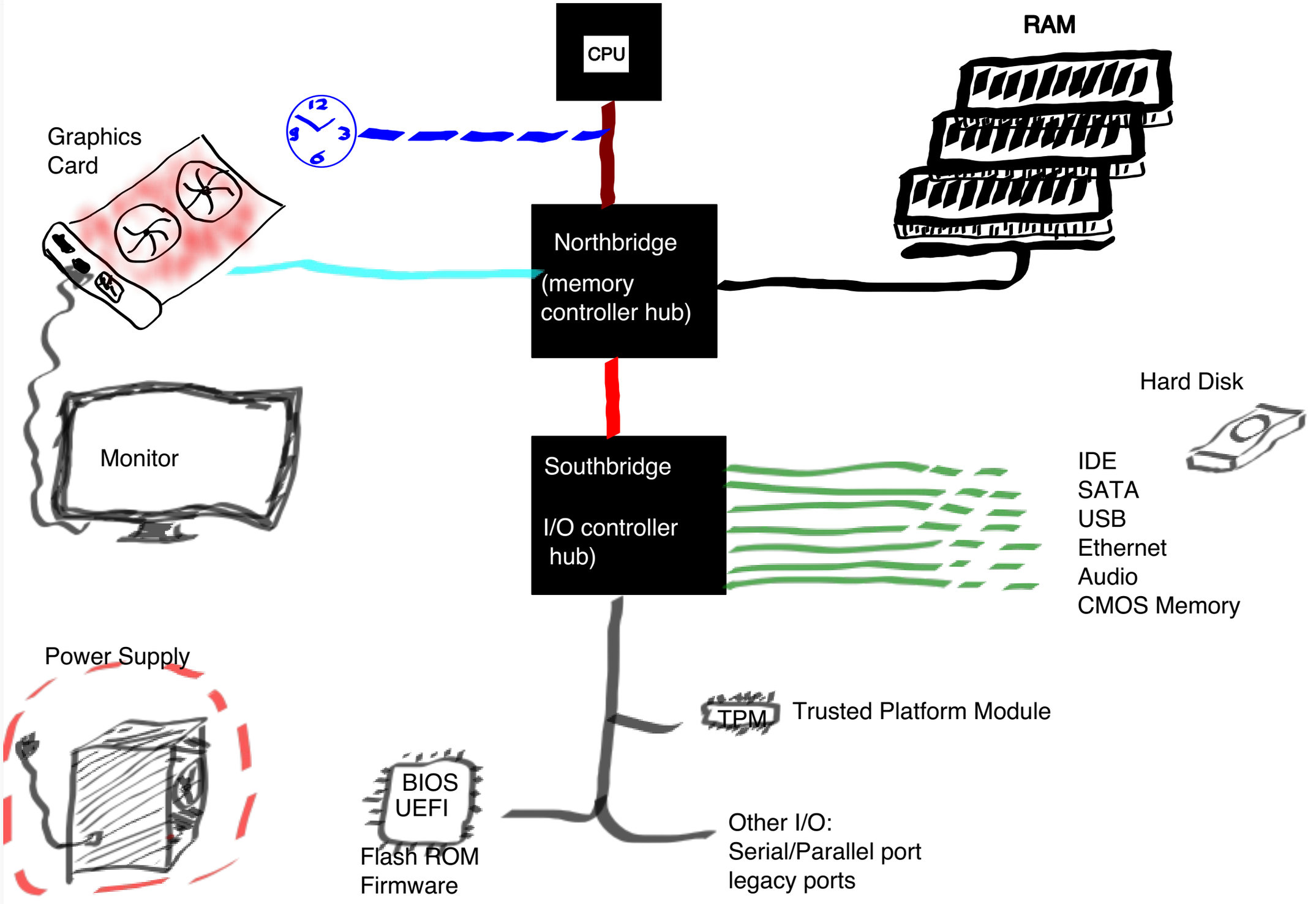
- Turn power on
- Power good?
- Start clock

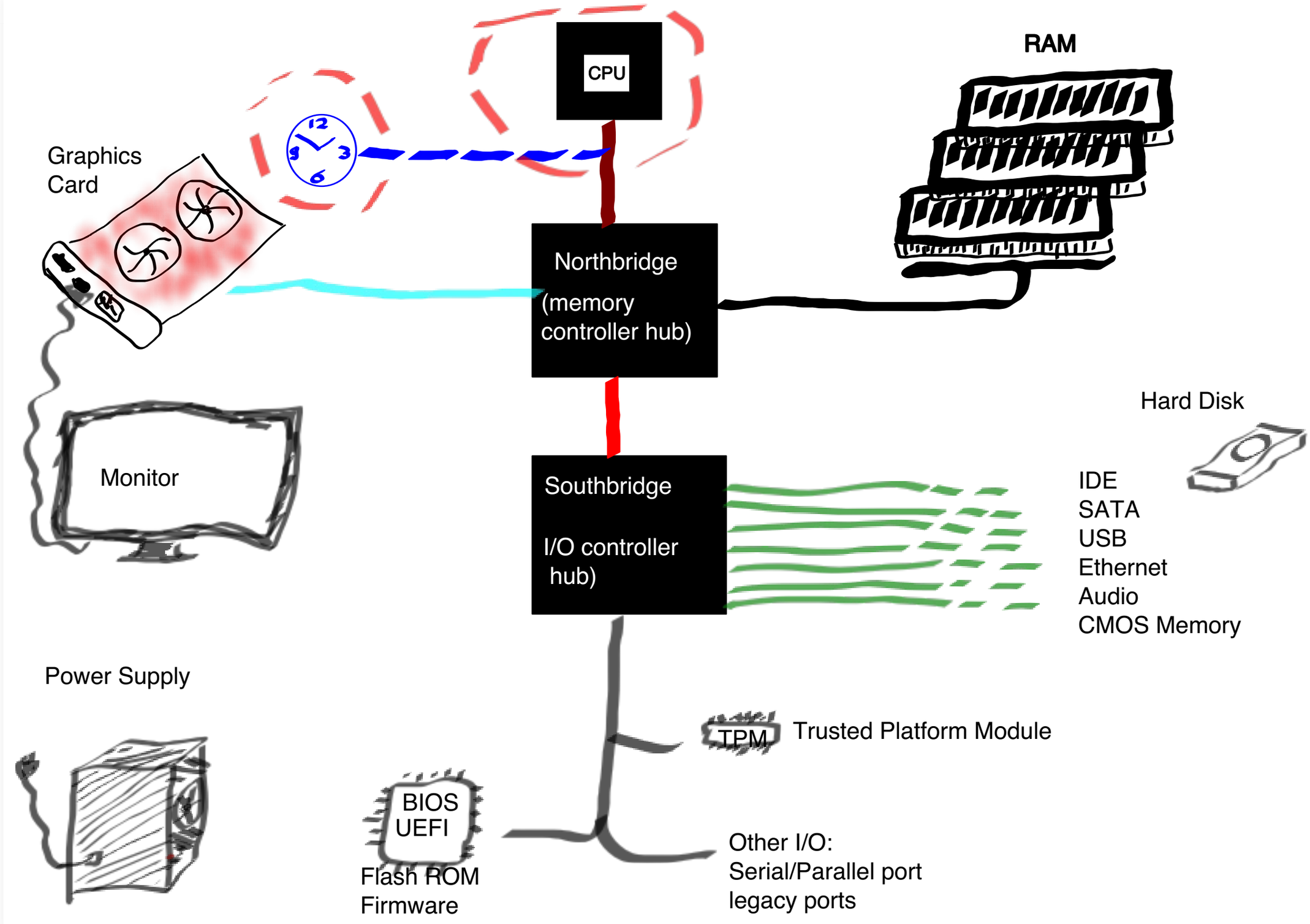
Boot process

- Turn power on
- Power good?
- Start clock
- Start fans (cooling)

Boot process

- Turn power on
- Power good?
- Start clock
- Start fans (cooling)
- Send Reset CPU signal


CPU
RAM
Graphics
Card
Northbridge
(memory
controller hub)
Monitor
Hard Disk
Southbridge
I/O controller
hub)
IDE
SATA
USB
Ethernet
Audio
CMOS Memory
Power Supply
TPM
Trusted Platform Module
BIOS
UEFI
Flash ROM
Firmware
Other I/O:
Serial/Parallel port
legacy ports


CPU
RAM
Graphics Card
Northbridge
(memory controller hub)
Monitor
Hard Disk
Southbridge
I/O controller hub)
IDE
SATA
USB
Ethernet
Audio
CMOS Memory
Power Supply
TPM
Trusted Platform Module
BIOS
UEFI
Flash ROM
Firmware
Other I/O:
Serial/Parallel port
legacy ports

Boot process

- Turn power on
- Power good?
- Start clock
- Start fans (cooling)
- Send Reset CPU signal

Boot process

- Turn power on
- Power good?
- Start clock
- Start fans (cooling)
- Send Reset CPU signal
- CPU can't do much without software

Initial software

Drivers are required for all hardware:

Initial software

Drivers are required for all hardware:

- Operating System (OS) stored on hard disk

Initial software

Drivers are required for all hardware:

- Operating System (OS) stored on hard disk
- Screen connected to graphics card

Initial software

Drivers are required for all hardware:

- Operating System (OS) stored on hard disk
- Screen connected to graphics card
- Keyboard, mouse connected via USB

Initial software

Drivers are required for all hardware:

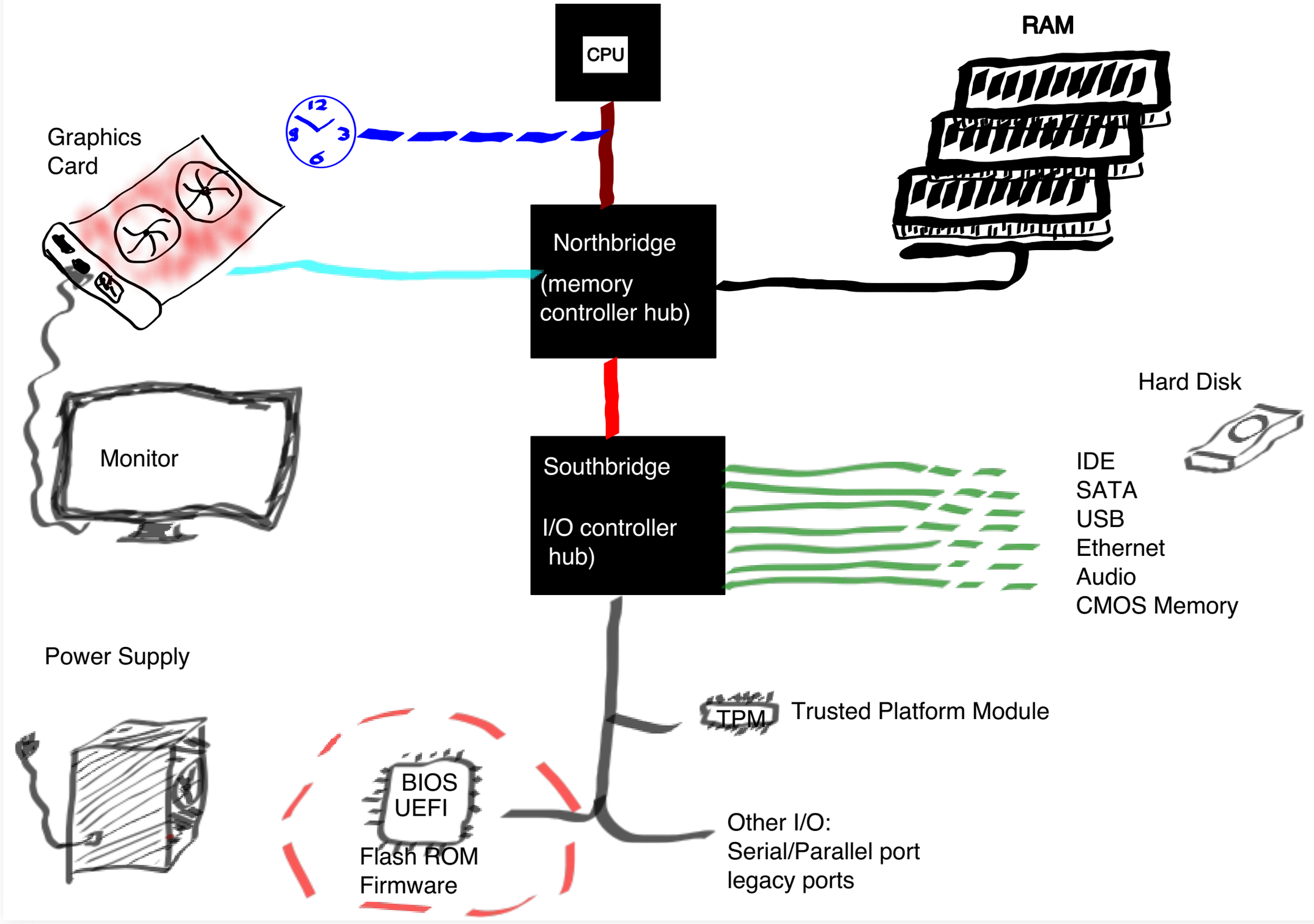
- Operating System (OS) stored on hard disk
- Screen connected to graphics card
- Keyboard, mouse connected via USB
- Network (WiFi, Ethernet)

Initial software

Drivers are required for all hardware:

- Operating System (OS) stored on hard disk
- Screen connected to graphics card
- Keyboard, mouse connected via USB
- Network (WiFi, Ethernet)

Booting must load software and activate hardware components in the right order.


CPU
RAM
Graphics Card
Northbridge
(memory controller hub)
Monitor
Hard Disk
Southbridge
I/O controller hub)
IDE
SATA
USB
Ethernet
Audio
CMOS Memory
Power Supply
TPM
Trusted Platform Module
BIOS
UEFI
Flash ROM
Firmware
Other I/O:
Serial/Parallel port
legacy ports

BIOS / UEFI

- BIOS (Basic Input Output System)
- UEFI (Unified Extensible Firmware Interface in modern PCs)

BIOS / UEFI

- BIOS (Basic Input Output System)
- UEFI (Unified Extensible Firmware Interface in modern PCs)
- stored in non-volatile memory (ROM - read only memory) on the motherboard

BIOS / UEFI

- BIOS (Basic Input Output System)
- UEFI (Unified Extensible Firmware Interface in modern PCs)
- stored in non-volatile memory (ROM - read only memory) on the motherboard
- controls the start-up steps

BIOS / UEFI

- BIOS (Basic Input Output System)
- UEFI (Unified Extensible Firmware Interface in modern PCs)
- stored in non-volatile memory (ROM - read only memory) on the motherboard
- controls the start-up steps
- provides initial system configuration (power saving, security, etc.)

BIOS / UEFI

- BIOS (Basic Input Output System)
- UEFI (Unified Extensible Firmware Interface in modern PCs)
- stored in non-volatile memory (ROM - read only memory) on the motherboard
- controls the start-up steps
- provides initial system configuration (power saving, security, etc.)
- initially configures some hardware

BIOS / UEFI

- The reset command in the CPU triggers the execution of an instruction at a specific location in the BIOS chip.
- Location contains a Jump instruction that points to the actual BIOS start-up program in the chip.
- Booting really starts with the execution of this start-up program.

Boot process: POST

BIOS starts with a power-on-self-test (POST):

Boot process: POST

BIOS starts with a power-on-self-test (POST):

- System memory is OK

Boot process: POST

BIOS starts with a power-on-self-test (POST):

- System memory is OK
- System clock / timer is running

Boot process: POST

BIOS starts with a power-on-self-test (POST):

- System memory is OK
- System clock / timer is running
- Processor is OK

Boot process: POST

BIOS starts with a power-on-self-test (POST):

- System memory is OK
- System clock / timer is running
- Processor is OK
- Keyboard is present

Boot process: POST

BIOS starts with a power-on-self-test (POST):

- System memory is OK
- System clock / timer is running
- Processor is OK
- Keyboard is present
- Screen display memory is working

Boot process: POST

BIOS starts with a power-on-self-test (POST):

- System memory is OK
- System clock / timer is running
- Processor is OK
- Keyboard is present
- Screen display memory is working
- BIOS is not corrupted

Boot process: POST

BIOS starts with a power-on-self-test (POST):

- System memory is OK
- System clock / timer is running
- Processor is OK
- Keyboard is present
- Screen display memory is working
- BIOS is not corrupted

Results of POST can only be communicated through system beep.

Boot process: Video card

- The first thing after a successful POST is to initialise the video card and show some initial message on the screen.
- Note that the BIOS can only do a rudimentary initialization. Use of 3D, fancy graphics, etc. needs additional software, the so-called driver.

```
Award Modular BIOS v6.00PG, An Energy Star Ally
Copyright (C) 1984-99, Award Software, Inc.

BIW1M/BIW2M BIOS V1.3

Main Processor : PENTIUM II 910MHz
Memory Testing :  131072K OK + 1024K Shared Memory

Award Plug and Play BIOS Extension v1.0A
Copyright (C) 1999, Award Software, Inc.

Trend ChipAwayVirus(R) On Guard Ver 1.64

Press DEL to enter SETUP, ALT+F2 to enter AWDFLASH
09/21/2000-i810-W83627HF-6A69MPNAC-00
```

Boot process: Other hardware

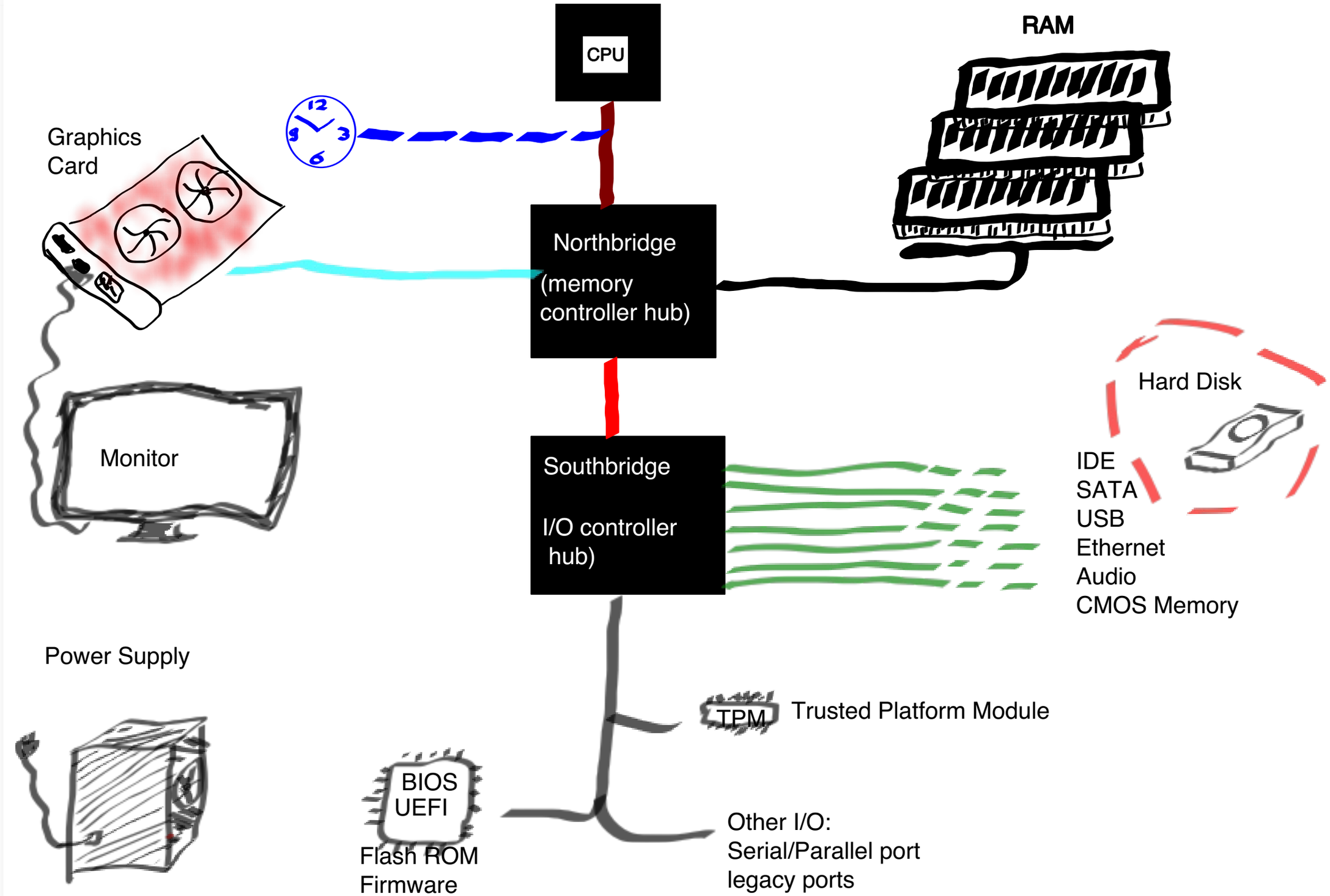
- Then, the BIOS goes through all available hardware and initializes as far as possible without more complex driver software (UEFI has more options)
- Examples are type and size of hard-disk, DVD drive, timing of RAM (random access memory) chips, networking, sound, etc.

Boot process: Find Operating System

- BIOS needs to look for a bootable drive
- Can be on a hard-disk, USB Stick, DVD, floppy disk,...
- Order is defined in BIOS configuration (usually accessible by holding a particular key while start-up screen is shown).

Boot process: Find Operating System

- BIOS needs to look for a bootable drive
- Can be on a hard-disk, USB Stick, DVD, floppy disk,...
- Order is defined in BIOS configuration (usually accessible by holding a particular key while start-up screen is shown).
- (Can even be over the network but we won't look at that option)

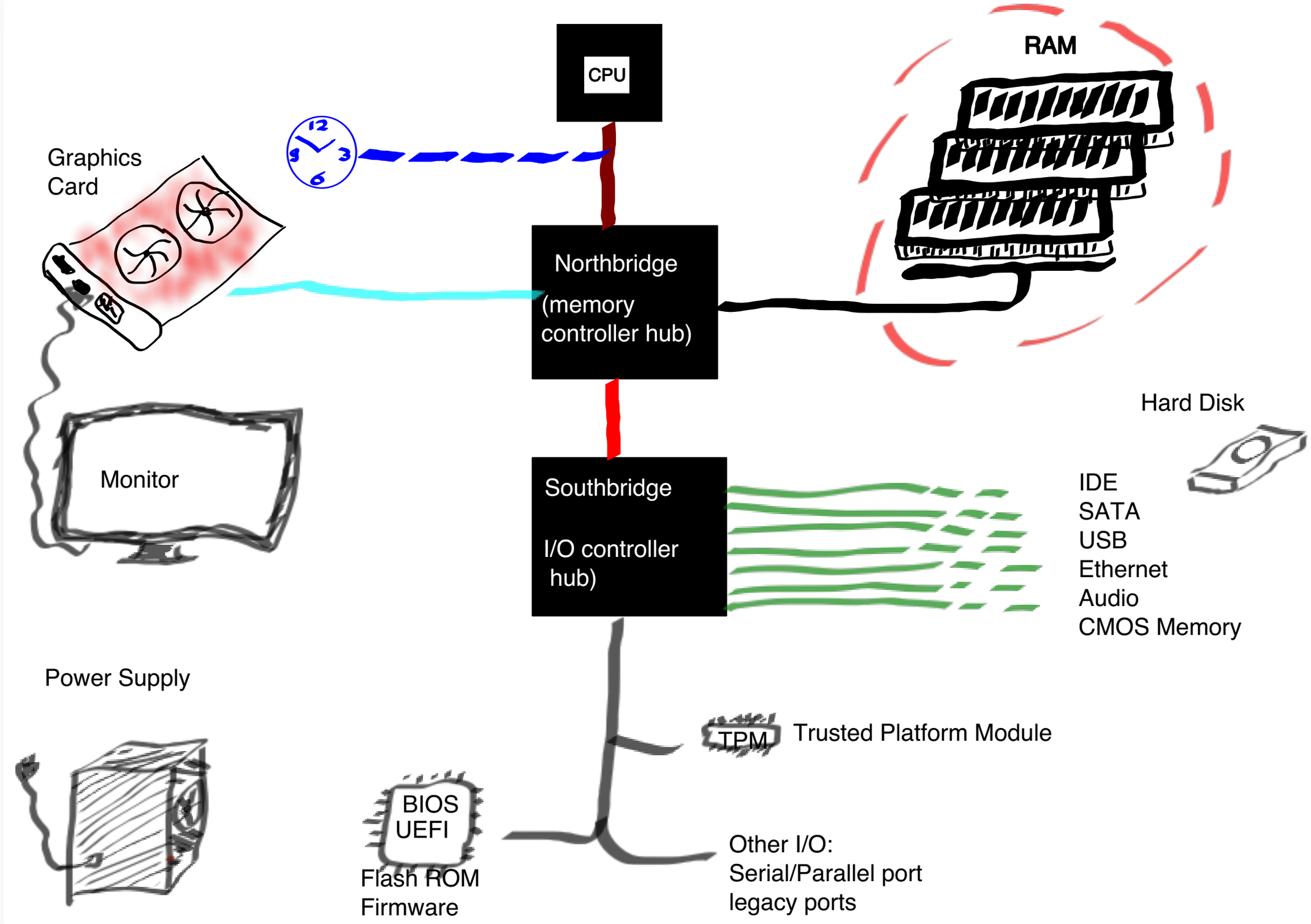

CPU
RAM
Graphics Card
Northbridge
(memory controller hub)
Monitor
Hard Disk
Southbridge
I/O controller hub)
IDE
SATA
USB
Ethernet
Audio
CMOS Memory
Power Supply
TPM
Trusted Platform Module
BIOS
UEFI
Flash ROM
Firmware
Other I/O:
Serial/Parallel port
legacy ports

Booting from disk

- Bootable drives have a boot sector:
  - contains executable code that loads the OS (boot loader)
  - stored in Master Boot Record (MBR) on hard disks
  - (sector just means a particular location on the disk)
- BIOS loads code from boot sector into RAM, then jumps into that code

Boot loader and kernel

- Loads the core part of the OS, the kernel, into RAM
- Jumps to start of kernel code
- Kernel loads various device drivers (e.g. for the graphics card).
- Once all drivers are loaded, the Graphical User interface (GUI) is started and personal settings are loaded.
- The computer is ready to use.


CPU
RAM
Graphics Card
Northbridge
(memory controller hub)
Monitor
Hard Disk
Southbridge
I/O controller hub)
IDE
SATA
USB
Ethernet
Audio
CMOS Memory
Power Supply
TPM
Trusted Platform Module
BIOS
UEFI
Flash ROM
Firmware
Other I/O:
Serial/Parallel port
legacy ports

BIOS disadvantages

BIOS is outdated

- Developed for 8088 processor (1983!)
- Intended as an abstraction layer for OS to access I/O (no longer used for this)
- Restricted to 1,024 kilobytes of space
- Only works with hard-drives up to 2.2 terabyte
- Cannot work with lots of current technology (and future technology)

UEFI

- Like a mini-operating system.
- Architecture-independent (e.g. available for x86 and ARM).
- Addresses some of the BIOS shortcomings.

UEFI

UEFI

- Can address hard-disks up to 9.4 zettabytes (1 zettabyte is about a billion terabytes).

UEFI

- Can address hard-disks up to 9.4 zettabytes (1 zettabyte is about a billion terabytes).
- Provides access to all hardware. Faster hardware initialization.

UEFI

- Can address hard-disks up to 9.4 zettabytes (1 zettabyte is about a billion terabytes).
- Provides access to all hardware. Faster hardware initialization.
- Can provide graphical user interface for configuration.

UEFI

- Can address hard-disks up to 9.4 zettabytes (1 zettabyte is about a billion terabytes).
- Provides access to all hardware. Faster hardware initialization.
- Can provide graphical user interface for configuration.
- Security and authentication features before the OS has started.

UEFI

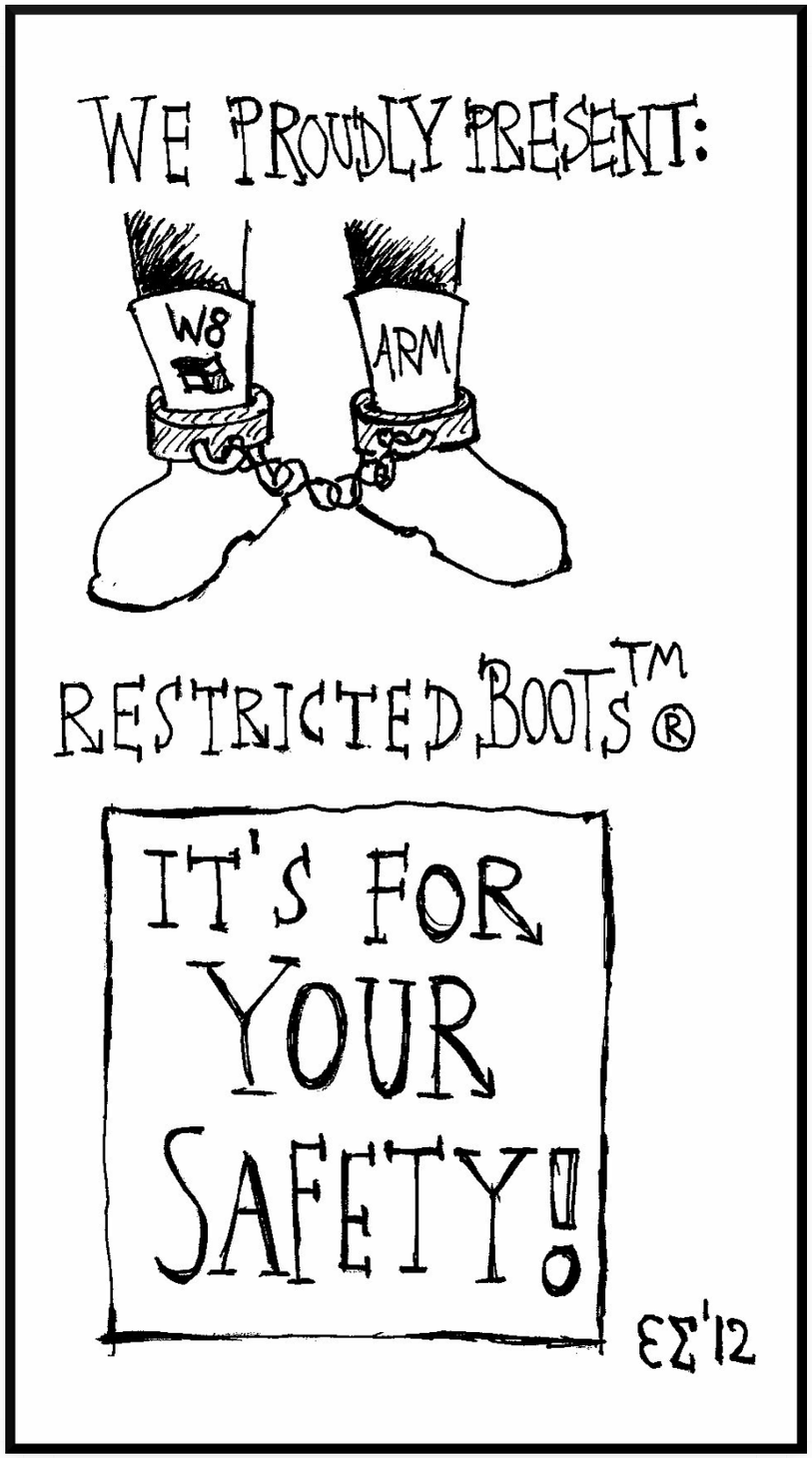
- Can address hard-disks up to 9.4 zettabytes (1 zettabyte is about a billion terabytes).
- Provides access to all hardware. Faster hardware initialization.
- Can provide graphical user interface for configuration.
- Security and authentication features before the OS has started.
- Network access before the OS has started.

UEFI

- Can address hard-disks up to 9.4 zettabytes (1 zettabyte is about a billion terabytes).
- Provides access to all hardware. Faster hardware initialization.
- Can provide graphical user interface for configuration.
- Security and authentication features before the OS has started.
- Network access before the OS has started.
- Remote administration before the OS has started.

UEFI criticism

- Boot restrictions (i.e. secure boot) can prevent users from installing the operating system of their choice.



Winner of "Restricted Boot" web comic, CC BY 3.0, By Erik Steinmann

UEFI criticism

- Boot restrictions (i.e. secure boot) can prevent users from installing the operating system of their choice.
- Additional complexity provides additional possibilities for errors and new attack vectors.

Most new PCs now use UEFI.

Some more on secure boot in the security part of the unit.

Next week

Operating systems