Libreboot Keynote

Paul Kocialkowski
contact@paulk.fr

Sunday June 5^{th} 2016

Freedom in Technology

Freedom in Technology

Computers and Freedom

Computers and Freedom Issues

Different computer types, form factors:

Computers and Freedom Issues

Different computer types, form factors:

- Desktops
- Laptops

Computers and Freedom Issues

Different computer types, form factors:

- Desktops
- Laptops
- Single-board computers

Computers and Freedom Issues

Different computer types, form factors:

- Desktops
- Laptops
- Single-board computers
- Mobile devices

Computers and Freedom Issues

Different computer types, form factors:

- Desktops
- Laptops
- Single-board computers
- Mobile devices

Issues:

Computers and Freedom Issues

Different computer types, form factors:

- Desktops
- Laptops
- Single-board computers
- Mobile devices

Issues:

- **Trust** in technology
  privacy/security implications

Computers and Freedom Issues

Different computer types, form factors:

- Desktops
- Laptops
- Single-board computers
- Mobile devices

Issues:

- **Trust** in technology
  privacy/security implications
- **Control** of the devices

Computers and Freedom Issues

Different computer types, form factors:

- Desktops
- Laptops
- Single-board computers
- Mobile devices

Issues:

- **Trust** in technology
  privacy/security implications
- **Control** of the devices
- **Knowledge** of the inner-workings,
  preservation

Basic Freedoms and Software

Guarantees: basic freedoms

1. Run for any purpose
2. Study and modify
3. Redistribution
4. Redistribution of modifications

Different forms of technology:

Basic Freedoms and Software

Guarantees: basic freedoms

1. Run for any purpose
2. Study and modify
3. Redistribution
4. Redistribution of modifications

Different forms of technology:

- **Software**: modifiable series of instructions

Basic Freedoms and Software

Guarantees: basic freedoms

1. Run for any purpose
2. Study and modify
3. Redistribution
4. Redistribution of modifications

Different forms of technology:

- **Software**: modifiable series of instructions
- **Hardware configuration**: modifiable logic behavior configuration

Basic Freedoms and Software

Guarantees: basic freedoms

1. Run for any purpose
2. Study and modify
3. Redistribution
4. Redistribution of modifications

Different forms of technology:

- **Software**: modifiable series of instructions
- **Hardware configuration**: modifiable logic behavior configuration
- **Hardware PCB and chip design**: electrical layout description

Freedom in Technology

Embracing Freedom

Embracing Freedom: Hardware

Basic freedoms and hardware:

Embracing Freedom: Hardware

Basic freedoms and hardware:

- Modifications, *source code* and design

Embracing Freedom: Hardware

Basic freedoms and hardware:

- Modifications, *source code* and design
- Formats and toolchains

Embracing Freedom: Hardware

Basic freedoms and hardware:

- Modifications, *source code* and design
- Formats and toolchains
- Costs and scale

Embracing Freedom: Hardware

Basic freedoms and hardware:

- Modifications, *source code* and design
- Formats and toolchains
- Costs and scale
- Infrastructure and trust

Embracing Freedom: Hardware

Basic freedoms and hardware:

- Modifications, *source code* and design
- Formats and toolchains
- Costs and scale
- Infrastructure and trust

Current situation:

Embracing Freedom: Hardware

Basic freedoms and hardware:

- Modifications, *source code* and design
- Formats and toolchains
- Costs and scale
- Infrastructure and trust

Current situation:

- Possible to some limited extent

Embracing Freedom: Hardware

Basic freedoms and hardware:

- Modifications, *source code* and design
- Formats and toolchains
- Costs and scale
- Infrastructure and trust

Current situation:

- Possible to some limited extent
- Free integrated circuit designs examples:
  OpenRISC, OpenSPARC, LEON, LM32, lowRISC, etc

Embracing Freedom: Hardware

Basic freedoms and hardware:

- Modifications, *source code* and design
- Formats and toolchains
- Costs and scale
- Infrastructure and trust

Current situation:

- Possible to some limited extent
- Free integrated circuit designs examples:
  OpenRISC, OpenSPARC, LEON, LM32, lowRISC, etc
- Free printed circuit board designs examples:
  Arduino, Freeduino, USB armory, Novena, etc

Embracing Freedom: Hardware

Basic freedoms and hardware:

- Modifications, *source code* and design
- Formats and toolchains
- Costs and scale
- Infrastructure and trust

Current situation:

- Possible to some limited extent
- Free integrated circuit designs examples:
  OpenRISC, OpenSPARC, LEON, LM32, lowRISC, etc
- Free printed circuit board designs examples:
  Arduino, Freeduino, USB armory, Novena, etc
- Documented hardware, "OpenHardware" confusion

Embracing Freedom: Hardware configuration

Different forms:

Embracing Freedom: Hardware configuration

Different forms:

- FPGA configuration

Embracing Freedom: Hardware configuration

Different forms:

- FPGA configuration
- CPU microcodes

Embracing Freedom: Hardware configuration

Different forms:

- FPGA configuration
- CPU microcodes

Current situation:

Embracing Freedom: Hardware configuration

Different forms:

- FPGA configuration
- CPU microcodes

Current situation:

- Read-only, pre-installed or loaded

Embracing Freedom: Hardware configuration

Different forms:

- FPGA configuration
- CPU microcodes

Current situation:

- Read-only, pre-installed or loaded
- Verification, signatures

Embracing Freedom: Hardware configuration

Different forms:

- FPGA configuration
- CPU microcodes

Current situation:

- Read-only, pre-installed or loaded
- Verification, signatures
- Nearly always **proprietary** (CPU microcodes)

Embracing Freedom: Hardware configuration

Different forms:

- FPGA configuration
- CPU microcodes

Current situation:

- Read-only, pre-installed or loaded
- Verification, signatures
- Nearly always **proprietary** (CPU microcodes)
- Very often **essential**

Embracing Freedom: Software

First steps to embracing free software:

Embracing Freedom: Software

First steps to embracing free software:

- Free system

Embracing Freedom: Software

First steps to embracing free software:

- Free system
- Compatible hardware

Embracing Freedom: Software

First steps to embracing free software:

- Free system
- Compatible hardware
- Spread among devices, form factors

Embracing Freedom: Software

First steps to embracing free software:

- Free system
- Compatible hardware
- Spread among devices, form factors

Software at the **lower levels**:

Embracing Freedom: Software

First steps to embracing free software:

- Free system
- Compatible hardware
- Spread among devices, form factors

Software at the **lower levels**:

- Bootup software

Embracing Freedom: Software

First steps to embracing free software:

- Free system
- Compatible hardware
- Spread among devices, form factors

Software at the **lower levels**:

- Bootup software
- Trusted software environment

Embracing Freedom: Software

First steps to embracing free software:

- Free system
- Compatible hardware
- Spread among devices, form factors

Software at the **lower levels**:

- Bootup software
- Trusted software environment
- Firmwares

Freedom in Technology

Status of Free Software at the Lower Levels

Firmwares

Found in various components:

Firmwares

Found in various components:

- Auxilary processors: GPU, VPU, DSP

Firmwares

Found in various components:

- Auxilary processors: GPU, VPU, DSP
- Controllers:

Firmwares

Found in various components:

- Auxilary processors: GPU, VPU, DSP
- Controllers:
  - Ethernet (NIC), USB 3 (xHCI)

Firmwares

Found in various components:

- Auxilary processors: GPU, VPU, DSP
- Controllers:
  - Ethernet (NIC), USB 3 (xHCI)
  - Storage (hard drivers, flash storage)

Firmwares

Found in various components:

- Auxilary processors: GPU, VPU, DSP
- Controllers:
  - Ethernet (NIC), USB 3 (xHCI)
  - Storage (hard drivers, flash storage)
  - Embedded controller (laptops)

Firmwares

Found in various components:

- Auxilary processors: GPU, VPU, DSP
- Controllers:
  - Ethernet (NIC), USB 3 (xHCI)
  - Storage (hard drivers, flash storage)
  - Embedded controller (laptops)
  - Very often using processors
- Peripherals:
  - Communications (Wi-Fi, WWAN, GPS)

Firmwares

Found in various components:

- Auxilary processors: GPU, VPU, DSP
- Controllers:
  - Ethernet (NIC), USB 3 (xHCI)
  - Storage (hard drivers, flash storage)
  - Embedded controller (laptops)
  - Very often using processors
- Peripherals:
  - Communications (Wi-Fi, WWAN, GPS)
  - Media treatment (webcam, etc)

Firmwares

Found in various components:

- Auxilary processors: GPU, VPU, DSP
- Controllers:
  - Ethernet (NIC), USB 3 (xHCI)
  - Storage (hard drivers, flash storage)
  - Embedded controller (laptops)
  - Very often using processors
- Peripherals:
  - Communications (Wi-Fi, WWAN, GPS)
  - Media treatment (webcam, etc)
  - Very often using processors

Firmwares and Freedom

Current situation:

- Read-only, pre-installed or loaded

Firmwares and Freedom

Current situation:

- Read-only, pre-installed or loaded
- Verification, signatures

Firmwares and Freedom

Current situation:

- Read-only, pre-installed or loaded
- Verification, signatures
- Nearly always **proprietary**

Firmwares and Freedom

Current situation:

- Read-only, pre-installed or loaded
- Verification, signatures
- Nearly always **proprietary**
- Cannot always be **avoided**, workaround

Firmwares and Freedom

Current situation:

- Read-only, pre-installed or loaded
- Verification, signatures
- Nearly always **proprietary**
- Cannot always be **avoided**, workaround

Free software support:

- Specific hardware (Arduino, BusPirate, FX2LA)
- Wi-Fi peripherals (ath9k_htc, AR9170, OpenFWWF)

Trusted Software Environment

Need for trusted software:

Trusted Software Environment

Need for trusted software:

- Operating system is flawed

Trusted Software Environment

Need for trusted software:

- Operating system is flawed
- Privileged operations, hardware access
- Sensitive operations (privacy/security)

Trusted Software Environment

Need for trusted software:

- Operating system is flawed
- Privileged operations, hardware access
- Sensitive operations (privacy/security)

Implementing a trusted software environment:

Trusted Software Environment

Need for trusted software:

- Operating system is flawed
- Privileged operations, hardware access
- Sensitive operations (privacy/security)

Implementing a trusted software environment:

- Cooperation with the chip (**TrustZone**)

Trusted Software Environment

Need for trusted software:

- Operating system is flawed
- Privileged operations, hardware access
- Sensitive operations (privacy/security)

Implementing a trusted software environment:

- Cooperation with the chip (**TrustZone**)
- Setup early (by bootup software)

Trusted Software Environment

Need for trusted software:

- Operating system is flawed
- Privileged operations, hardware access
- Sensitive operations (privacy/security)

Implementing a trusted software environment:

- Cooperation with the chip (**TrustZone**)
- Setup early (by bootup software)
- Privileged mode, Secure Monitor Call (SMC)

Trusted Software Environment and Freedom

Consequences for freedom:

Trusted Software Environment and Freedom

Consequences for freedom:

- Not good or bad *per-se*
- Most privileged software
- **Privacy/security** implications

Trusted Software Environment and Freedom

Consequences for freedom:

- Not good or bad *per-se*
- Most privileged software
- **Privacy/security** implications
- Free software implementations

Trusted Software Environment and Freedom

Consequences for freedom:

- Not good or bad *per-se*
- Most privileged software
- **Privacy/security** implications
- Free software implementations
- Dependence on the bootloader situation
- **Proprietary** and **verified** implementations (recent devices)
- Known good examples: USB armory with i.MX53, Rockchip

Trusted Software Environment and Freedom

Consequences for freedom:

- Not good or bad *per-se*
- Most privileged software
- **Privacy/security** implications
- Free software implementations
- Dependence on the bootloader situation
- **Proprietary** and **verified** implementations (recent devices)
- Known good examples: USB armory with i.MX53, Rockchip

Often problematic on recent devices, but could be done right

Bootup Software

Boot chain:

Bootup Software

Boot chain:

- (Bootrom)

Bootup Software

Boot chain:

- (Bootrom)
- Hardware initialization

Bootup Software

Boot chain:

- (Bootrom)
- Hardware initialization
- Bootloader, payload

Bootup Software

Boot chain:

- (Bootrom)
- Hardware initialization
- Bootloader, payload

Implications of a bootrom:

- **Proprietary**, read-only memory (hardware-like)

Bootup Software

Boot chain:

- (Bootrom)
- Hardware initialization
- Bootloader, payload

Implications of a bootrom:

- **Proprietary**, read-only memory (hardware-like)
- Verification with **signatures**, chain of trust
  platform-specific, specific models
- Boot media selection, reflashing

Bootup Software and Freedom

BIOS implementations:

Bootup Software and Freedom

BIOS implementations:

- Historically **non-free**

Bootup Software and Freedom

BIOS implementations:

- Historically **non-free**
- Individual interest, LinuxBIOS (2000)

Bootup Software and Freedom

BIOS implementations:

- Historically **non-free**
- Individual interest, LinuxBIOS (2000)
- Renamed to **Coreboot**, 2008

Bootup Software and Freedom

BIOS implementations:

- Historically **non-free**
- Individual interest, LinuxBIOS (2000)
- Renamed to **Coreboot**, 2008
- **Non-free** blobs introduction:

Bootup Software and Freedom

BIOS implementations:

- Historically **non-free**
- Individual interest, LinuxBIOS (2000)
- Renamed to **Coreboot**, 2008
- **Non-free** blobs introduction:
  - Option ROM/VGA BIOS

Bootup Software and Freedom

BIOS implementations:

- Historically **non-free**
- Individual interest, LinuxBIOS (2000)
- Renamed to **Coreboot**, 2008
- **Non-free** blobs introduction:
  - Option ROM/VGA BIOS
  - CPU microcodes

Bootup Software and Freedom

BIOS implementations:

- Historically **non-free**
- Individual interest, LinuxBIOS (2000)
- Renamed to **Coreboot**, 2008
- **Non-free** blobs introduction:
  - Option ROM/VGA BIOS
  - CPU microcodes
  - Hardware initialization

Bootup Software and Freedom

BIOS implementations:

- Historically **non-free**
- Individual interest, LinuxBIOS (2000)
- Renamed to **Coreboot**, 2008
- **Non-free** blobs introduction:
  - Option ROM/VGA BIOS
  - CPU microcodes
  - Hardware initialization
  - Firmwares

Bootup Software and Freedom

BIOS implementations:

- Historically **non-free**
- Individual interest, LinuxBIOS (2000)
- Renamed to **Coreboot**, 2008
- **Non-free** blobs introduction:
  - Option ROM/VGA BIOS
  - CPU microcodes
  - Hardware initialization
  - Firmwares

Non-x86 embedded devices:

Bootup Software and Freedom

BIOS implementations:

- Historically **non-free**
- Individual interest, LinuxBIOS (2000)
- Renamed to **Coreboot**, 2008
- **Non-free** blobs introduction:
  - Option ROM/VGA BIOS
  - CPU microcodes
  - Hardware initialization
  - Firmwares

Non-x86 embedded devices:

- Free software projects: **U-Boot**, **Barebox**

Bootup Software and Freedom

BIOS implementations:

- Historically **non-free**
- Individual interest, LinuxBIOS (2000)
- Renamed to **Coreboot**, 2008
- **Non-free** blobs introduction:
  - Option ROM/VGA BIOS
  - CPU microcodes
  - Hardware initialization
  - Firmwares

Non-x86 embedded devices:

- Free software projects: **U-Boot**, **Barebox**
- Reference and use

Bootup Software and Freedom

BIOS implementations:

- Historically **non-free**
- Individual interest, LinuxBIOS (2000)
- Renamed to **Coreboot**, 2008
- **Non-free** blobs introduction:
  - Option ROM/VGA BIOS
  - CPU microcodes
  - Hardware initialization
  - Firmwares

Non-x86 embedded devices:

- Free software projects: **U-Boot**, **Barebox**
- Reference and use
- Similar **non-free** blobs

Bootup Software and Freedom

Many supported devices, with blobs!

First laptops working without blobs (2013):

- x60/t60 laptops
- Graphics initialization

Bootup Software and Freedom

Many supported devices, with blobs!

First laptops working without blobs (2013):

- x60/t60 laptops
- Graphics initialization
- Libreboot project

Bootup Software and Freedom

Many supported devices, with blobs!

First laptops working without blobs (2013):

- x60/t60 laptops
- Graphics initialization
- Libreboot project
- Devices distribution: Gluglug, Minifree

Libreboot

Libreboot

Project Presentation

Libreboot Presentation

Aim and focus:

Libreboot Presentation

Aim and focus:

- Fully free bootup software

Libreboot Presentation

Aim and focus:

- Fully free bootup software
- Distribution of Coreboot

Libreboot Presentation

Aim and focus:

- Fully free bootup software
- Distribution of Coreboot
- GNU project since May 2016

Libreboot Presentation

Aim and focus:

- Fully free bootup software
- Distribution of Coreboot
- GNU project since May 2016

Technical side:

- Build system (Coreboot, tools)

Libreboot Presentation

Aim and focus:

- Fully free bootup software
- Distribution of Coreboot
- GNU project since May 2016

Technical side:

- Build system (Coreboot, tools)
- Configuration for supported devices

Libreboot Presentation

Aim and focus:

- Fully free bootup software
- Distribution of Coreboot
- GNU project since May 2016

Technical side:

- Build system (Coreboot, tools)
- Configuration for supported devices
- Images releases

Libreboot Presentation

Aim and focus:

- Fully free bootup software
- Distribution of Coreboot
- GNU project since May 2016

Technical side:

- Build system (Coreboot, tools)
- Configuration for supported devices
- Images releases
- Documentation, instructions

Supported Devices

Laptops:

- x60, t60, x200, r400, t400, t500 laptops
- Macbook 1.1, 1.2
- CrOS devices (chromebook laptops)

Supported Devices

Laptops:

- x60, t60, x200, r400, t400, t500 laptops
- Macbook 1.1, 1.2
- CrOS devices (chromebook laptops)

Desktop motherboards:

- Gigabyte GA-G41M-ES2L
- Intel D510MO
- ASUS KCMA-D8

Supported Devices

Laptops:

- x60, t60, x200, r400, t400, t500 laptops
- Macbook 1.1, 1.2
- CrOS devices (chromebook laptops)

Desktop motherboards:

- Gigabyte GA-G41M-ES2L
- Intel D510MO
- ASUS KCMA-D8

Server motherboards:

- ASUS KFSN4-DRE
- ASUS KGPE-D16

Libreboot

x86 Platforms Case Studies

Intel x86 platforms

Intel x86 platforms evaluation:

Intel x86 platforms

Intel x86 platforms evaluation:

- Intel Management Engine (ME)

Intel x86 platforms

Intel x86 platforms evaluation:

- Intel Management Engine (ME)
- Firmware Support Package (FSP)

Intel x86 platforms

Intel x86 platforms evaluation:

- Intel Management Engine (ME)
- Firmware Support Package (FSP)
- xHCI firmware

Intel x86 platforms

Intel x86 platforms evaluation:

- Intel Management Engine (ME)
- Firmware Support Package (FSP)
- xHCI firmware
- GPU firmware

Intel x86 platforms

Intel x86 platforms evaluation:

- Intel Management Engine (ME)
- Firmware Support Package (FSP)
- xHCI firmware
- GPU firmware
- CPU microcode and updates

Intel x86 platforms

Intel x86 platforms evaluation:

- Intel Management Engine (ME)
- Firmware Support Package (FSP)
- xHCI firmware
- GPU firmware
- CPU microcode and updates
- Intel is uncooperative

AMD x86 platforms

AMD x86 platforms evaluation:

AMD x86 platforms

AMD x86 platforms evaluation:

- Platform Security Processor (PSP)

AMD x86 platforms

AMD x86 platforms evaluation:

- Platform Security Processor (PSP)
- IMC firmware

AMD x86 platforms

AMD x86 platforms evaluation:

- Platform Security Processor (PSP)
- IMC firmware
- SMU firmware

AMD x86 platforms

AMD x86 platforms evaluation:

- Platform Security Processor (PSP)
- IMC firmware
- SMU firmware
- AGESA firmware

AMD x86 platforms

AMD x86 platforms evaluation:

- Platform Security Processor (PSP)
- IMC firmware
- SMU firmware
- AGESA firmware
- xHCI firmware

AMD x86 platforms

AMD x86 platforms evaluation:

- Platform Security Processor (PSP)
- IMC firmware
- SMU firmware
- AGESA firmware
- xHCI firmware
- GPU firmware and initialization

AMD x86 platforms

AMD x86 platforms evaluation:

- Platform Security Processor (PSP)
- IMC firmware
- SMU firmware
- AGESA firmware
- xHCI firmware
- GPU firmware and initialization
- CPU microcode updates

AMD x86 platforms

AMD x86 platforms evaluation:

- Platform Security Processor (PSP)
- IMC firmware
- SMU firmware
- AGESA firmware
- xHCI firmware
- GPU firmware and initialization
- CPU microcode updates
- AMD is uncooperative

Various ARM and MIPS platforms

ARM and MIPS platforms evaluation:

Various ARM and MIPS platforms

ARM and MIPS platforms evaluation:

- Bootrom, verification

Various ARM and MIPS platforms

ARM and MIPS platforms evaluation:

- Bootrom, verification
- Trusted firmware environment

Various ARM and MIPS platforms

ARM and MIPS platforms evaluation:

- Bootrom, verification
- Trusted firmware environment
- Auxiliary processors firmware

Various ARM and MIPS platforms

ARM and MIPS platforms evaluation:

- Bootrom, verification
- Trusted firmware environment
- Auxiliary processors firmware
- xHCI firmware

Various ARM and MIPS platforms

ARM and MIPS platforms evaluation:

- Bootrom, verification
- Trusted firmware environment
- Auxiliary processors firmware
- xHCI firmware
- CPU microcodes

Various ARM and MIPS platforms

ARM and MIPS platforms evaluation:

- Bootrom, verification
- Trusted firmware environment
- Auxiliary processors firmware
- xHCI firmware
- CPU microcodes
- Free operating systems support

POWER8 platforms

POWER8 platforms evaluation:

POWER8 platforms

POWER8 platforms evaluation:

- Bootup software

POWER8 platforms

POWER8 platforms evaluation:

- Bootup software
- Baseboard Management Controller system

POWER8 platforms

POWER8 platforms evaluation:

- Bootup software
- Baseboard Management Controller system
- CPU microcodes, updates?

POWER8 platforms

POWER8 platforms evaluation:

- Bootup software
- Baseboard Management Controller system
- CPU microcodes, updates?
- Free operating systems support

POWER8 platforms

POWER8 platforms evaluation:

- Bootup software
- Baseboard Management Controller system
- CPU microcodes, updates?
- Free operating systems support
- IBM, OpenPOWER foundation

Raptor Engineering TALOS workstation
https://raptorengineering.com/TALOS/

Libreboot

Supported Devices Case Studies

x60, t60, x200, r400, t400, t500, Macbook Laptops

Platform-specific aspects:

x60, t60, x200, r400, t400, t500, Macbook Laptops

Platform-specific aspects:

- Management Engine

x60, t60, x200, r400, t400, t500, Macbook Laptops

Platform-specific aspects:

- Management Engine
- Hardware initialization

x60, t60, x200, r400, t400, t500, Macbook Laptops

Platform-specific aspects:

- Management Engine
- Hardware initialization
- CPU microcode and updates

Proprietary firmwares:

x60, t60, x200, r400, t400, t500, Macbook Laptops

Platform-specific aspects:

- Management Engine
- Hardware initialization
- CPU microcode and updates

Proprietary firmwares:

- Embedded Controller (EC)

x60, t60, x200, r400, t400, t500, Macbook Laptops

Platform-specific aspects:

- Management Engine
- Hardware initialization
- CPU microcode and updates

Proprietary firmwares:

- Embedded Controller (EC)
- Hard drive controller

x60, t60, x200, r400, t400, t500, Macbook Laptops

Platform-specific aspects:

- Management Engine
- Hardware initialization
- CPU microcode and updates

Proprietary firmwares:

- Embedded Controller (EC)
- Hard drive controller
- Various peripherals (battery, webcam, etc)

CrOS Devices (Chromebook Laptops)

Factory hardware and software:

CrOS Devices (Chromebook Laptops)

Factory hardware and software:

- Downstream Coreboot, Depthcharge

CrOS Devices (Chromebook Laptops)

Factory hardware and software:

- Downstream Coreboot, Depthcharge
- Embedded Controller firmware

CrOS Devices (Chromebook Laptops)

Factory hardware and software:

- Downstream Coreboot, Depthcharge
- Embedded Controller firmware
- Security model

CrOS Devices (Chromebook Laptops)

Factory hardware and software:

- Downstream Coreboot, Depthcharge
- Embedded Controller firmware
- Security model
- The screw, flashing tools

CrOS Devices (Chromebook Laptops)

Factory hardware and software:

- Downstream Coreboot, Depthcharge
- Embedded Controller firmware
- Security model
- The screw, flashing tools
- ChromeOS

CrOS Devices (Chromebook Laptops)

Factory hardware and software:

- Downstream Coreboot, Depthcharge
- Embedded Controller firmware
- Security model
- The screw, flashing tools
- ChromeOS

Supported platforms (CrOS devices):

CrOS Devices (Chromebook Laptops)

Factory hardware and software:

- Downstream Coreboot, Depthcharge
- Embedded Controller firmware
- Security model
- The screw, flashing tools
- ChromeOS

Supported platforms (CrOS devices):

- Recent Intel

CrOS Devices (Chromebook Laptops)

Factory hardware and software:

- Downstream Coreboot, Depthcharge
- Embedded Controller firmware
- Security model
- The screw, flashing tools
- ChromeOS

Supported platforms (CrOS devices):

- Recent Intel
- ARM (Tegra K1, RK3288)

Proprietary firmwares:

CrOS Devices (Chromebook Laptops)

Factory hardware and software:

- Downstream Coreboot, Depthcharge
- Embedded Controller firmware
- Security model
- The screw, flashing tools
- ChromeOS

Supported platforms (CrOS devices):

- Recent Intel
- ARM (Tegra K1, RK3288)

Proprietary firmwares:

- Platform-specific firmwares (xHCI, video decoding)

CrOS Devices (Chromebook Laptops)

Factory hardware and software:

- Downstream Coreboot, Depthcharge
- Embedded Controller firmware
- Security model
- The screw, flashing tools
- ChromeOS

Supported platforms (CrOS devices):

- Recent Intel
- ARM (Tegra K1, RK3288)

Proprietary firmwares:

- Platform-specific firmwares (xHCI, video decoding)
- Flash storage (eMMC) controller

CrOS Devices (Chromebook Laptops)

Factory hardware and software:

- Downstream Coreboot, Depthcharge
- Embedded Controller firmware
- Security model
- The screw, flashing tools
- ChromeOS

Supported platforms (CrOS devices):

- Recent Intel
- ARM (Tegra K1, RK3288)

Proprietary firmwares:

- Platform-specific firmwares (xHCI, video decoding)
- Flash storage (eMMC) controller
- Various peripherals (battery, webcam, etc)

Learn more about Libreboot:

- Website: **https://libreboot.org/**

Join the community:

- Mailing lists: **libreboot**, **libreboot-dev** at **gnu.org**
- IRC channel: **#libreboot** at **Freenode**

The project needs help!

- More hardware to support!
- **Donations** are welcome (devices are expensive)