# Hardware Hacking Introduction - Overview

Joas Antonio

# Details

- This PDF is just an overview of Hardware Hacking, for those who are looking for content for study and development in the area.
- https://www.linkedin.com/in/joas-antonio-dos-santos

# Introduction

https://www.linkedin.com/in/joas-antonio-dos-santos

# Importance

- Hardware hacking skills are an emerging skill set that can open a good opportunity for one’s career. It can also be considered a hobby for hunting down the electrons, which can truly kill your pastimes. In brief, we can say that it is the best of its kind. Below are the important features of Hardware Hacking:

https://www.educba.com/hardware-hacking/

# Importance

- **Hands-on Experience:** this is the most important feature that adds beauty to Hardware hacking is that not only theoretical knowledge but also hands-on experience in building or hacking up electronics. This is the major difference between Hardware and software hacking.
- **Endless Possibilities:** we are surrounded by endless hardware devices to hack only if we have permission to do so. There is n number of things on which we can hack, such as on LED bulbs, a computer's CPU, etc.
- **More Tangible:** you can feel the change physically once you hack any device. However, there are ups and downs in this case. We need to be quite careful in doing such things as it might kill your life. But in real life, the ability to interact physically with your work can be refreshing.
- **Digital Forensics:** There will be a need for hardware hacking when a device is partially destroyed, where forensics would need to interfere with few components to recover the evidence directly.
- **Testing**: Once the Hardware Devices are hacked, we can manually test them if they are working as per the required requirements. We can also bypass some software limitations to recover any electronic device by hardware hacking to dump private evidence from the device.
- **Programming Skills:** Hardware Hackers do have programming skills similar to software Hackers. Their knowledge of software Programming is more of a low level.  This basic understanding of software is pretty well used while Hardware hacking.

# Concepts 1 – Digital Eletronics

- https://pt.wikipedia.org/wiki/Circuito_digital
- https://en.wikipedia.org/wiki/Digital_electronics
- https://www.sciencedirect.com/topics/engineering/digital-circuits
- https://www.sciencedirect.com/topics/computer-science/digital-circuit
- https://www.youtube.com/watch?v=pyFyUsAeYPQ
- https://www.youtube.com/watch?v=esAE1WLAubM
- https://www.youtube.com/watch?v=kOckxSxf6XQ

# Concepts 2 – PCB

- https://www.pcbtrain.co.uk/blog/the-basics-of-printed-circuit-boards-design-components-and-construction
- https://www.ourpcb.com/pcb-components.html
- https://www.seeedstudio.com/blog/2019/06/12/12-commonly-used-components-on-pcbs-for-beginners/
- https://en.wikipedia.org/wiki/Printed_circuit_board
- https://www.protoexpress.com/pcb/learn-pcb/an-overview-of-basic-electronic-components/
- https://learn.sparkfun.com/tutorials/pcb-basics/all
- https://www.ablcircuits.co.uk/pcb-components/
- https://www.circuitspecialists.com/blog/commonly-used-components-on-pcbs/
- https://www.proto-electronics.com/blog/placements-of-components-pcb

# Concepts 3 – UART

- https://www.circuitbasics.com/basics-uart-communication/
- https://www.youtube.com/watch?v=sTHckUyxwp8
- https://www.youtube.com/watch?v=ZzRXKDkMBhA
- https://www.youtube.com/watch?v=IyGwvGzrqp8
- https://en.wikipedia.org/wiki/Universal_asynchronous_receiver-transmitter
- https://www.codrey.com/embedded-systems/uart-serial-communication-rs232/
- https://www.arrow.com/en/research-and-events/articles/what-is-uart-protocol-uart-communication-explained
- https://cs140e.sergio.bz/notes/lec4/uart-basics.pdf
- https://www.analog.com/en/analog-dialogue/articles/uart-a-hardware-communication-protocol.html
- https://www.electronicshub.org/basics-uart-communication/

# Concepts 4 – SPI Driver

- https://spidriver.com/
- https://01.org/linuxgraphics/gfx-docs/drm/driver-api/spi.html
- https://www.embarcados.com.br/comunicacao-spi-em-linux/
- https://www.youtube.com/watch?v=7F5TGZleOgw
- https://www.youtube.com/watch?v=ZmdQwpXlMw8
- https://www.nxp.com/docs/en/application-note/AN4162.pdf
- https://www.kernel.org/doc/html/v4.14/driver-api/spi.html
- https://wiki.st.com/stm32mpu/wiki/SPI_overview
- https://www.seeedstudio.com/SPI-Driver-Adapter-Easily-Driver-SPI-Devices-p-4023.html

# Concepts 5 – JTAG and SWD (CPU Debug)

- https://embeddedinventor.com/swd-vs-jtag-differences-explained/
- https://qastack.com.br/electronics/53571/jtag-vs-swd-debugging
- https://electronics.stackexchange.com/questions/53571/jtag-vs-swd-debugging
- https://research.kudelskisecurity.com/2019/05/16/swd-arms-alternative-to-jtag/
- https://learn.sparkfun.com/tutorials/arm-programming/jtag-and-swd
- https://www.keil.com/support/man/docs/ulinkplus/ulinkplus_jtagswd_interface.htm
- https://www.segger.com/products/debug-probes/j-link/technology/interface-description/
- https://www.sciencedirect.com/topics/computer-science/debug-interface
- https://community.silabs.com/s/article/serial-wire-debug-swd-x?language=en_US
- https://www.avrfreaks.net/forum/debugging-protocol-cpu-generated-pdi
- https://en.wikipedia.org/wiki/Nexus_(standard)
- https://www.jtag.com/jtag-hw-debugger/

# Concepts 6 – Firmware

- https://www.concept2.com/service/monitors/pm5/firmware
- https://en.wikipedia.org/wiki/Firmware
- https://techterms.com/definition/firmware
- https://courses.lumenlearning.com/zeliite115/chapter/reading-firmware/
- https://www.techopedia.com/definition/2137/firmware
- https://www.techslang.com/definition/what-is-firmware-in-computer/
- https://whatis.techtarget.com/definition/firmware
- https://www.youtube.com/watch?v=-R_RKlNfOFM
- https://www.youtube.com/watch?v=ZefOVNcz3ow
- https://www.youtube.com/watch?v=KkF9iopHF9o
- https://www.computerhope.com/jargon/f/firmware.htm

# Concepts 7 – i2c

- https://www.circuitbasics.com/basics-of-the-i2c-communication-protocol/
- https://pt.wikipedia.org/wiki/I%C2%B2C
- https://www.youtube.com/watch?v=6IAkYpmA1DQ
- https://www.youtube.com/watch?v=qTLRRg6Mee0
- https://www.youtube.com/watch?v=DsSBTYbXAKg
- https://learn.sparkfun.com/tutorials/i2c/all
- https://en.wikipedia.org/wiki/I%C2%B2C
- https://www.geeksforgeeks.org/i2c-communication-protocol/
- https://www.ti.com/lit/an/slva704/slva704.pdf?ts=1627996239307&ref_url=https%253A%252F%252Fwww.google.com%252F

# Concepts 8 – Arduino

- https://pt.wikipedia.org/wiki/Arduino#:~:text=Arduino%20%C3%A9%20uma%20plataforma%20de,%C3%A9%20essencialmente%20C%2FC%2B%2B.
- https://www.arduino.cc/en/guide/introduction
- https://learn.sparkfun.com/tutorials/what-is-an-arduino/all
- https://en.wikipedia.org/wiki/Arduino
- https://www.programmingelectronics.com/what-is-arduino/
- https://www.seeedstudio.com/blog/2019/12/04/introduction-to-the-arduino-what-is-arduino/
- https://www.techopedia.com/definition/27874/arduino
- https://www.rs-online.com/designspark/basics-of-arduino-uno
- https://www.electronicsmedia.info/2019/02/01/basic-concept-arduino-hardware-structure-arduino/
- https://www.youtube.com/watch?v=Pd754nSIr_E
- https://www.growthallianceevv.com/events/sensors-servos-arduino-basic-concept-course-jul-29-2021
- https://ieeexplore.ieee.org/abstract/document/8783256

# Concepts 9 – MCU

- https://internetofthingsagenda.techtarget.com/definition/microcontroller
- https://www.allaboutcircuits.com/technical-articles/what-is-a-microcontroller-introduction-component-characteristics-component/
- https://en.wikipedia.org/wiki/Microcontroller
- https://www.techopedia.com/definition/3641/microcontroller
- https://uk.rs-online.com/web/generalDisplay.html?id=ideas-and-advice/microcontrollers-guide
- https://www.arrow.com/en/research-and-events/articles/engineering-basics-what-is-a-microcontroller
- https://www.researchgate.net/publication/322436662_Understanding_the_Concept_of_Microcontroller_Based_Systems_To_Choose_The_Best_Hardware_For_Applications
- https://www.merriam-webster.com/dictionary/microcontroller
- https://www.theengineeringprojects.com/2018/03/introduction-to-microcontrollers.html

# Concepts 10 – Computer Architecture

- https://www.youtube.com/watch?v=MMiUBlxw6eU&list=PLL8bstVVO1fBU-TbAzjNqMHDYz8VwZQyc
- https://en.wikipedia.org/wiki/Computer_architecture ]
- https://www.archisoup.com/best-computers-for-architecture-students-and-architects
- https://www.oreilly.com/library/view/designing-embedded-hardware/0596007558/ch01.html
- https://architizer.com/blog/practice/tools/10-top-workstations-for-architects-and-designers/

# Concepts 11 – Hardware Hacking Kits

- https://www.tinkerforge.com/en/shop/kits/starter-kit-hardware-hacking.html
- https://www.youtube.com/watch?v=er0QfqjygBk
- https://www.youtube.com/watch?v=cHy0vUC2wzg
- https://danieldonda.com/wp-content/uploads/2020/06/FERRAMENTAS-PARA-HARDWARE-HACKING-danieldonda.com_.pdf
- https://www.sparkfun.com/wish_lists/155663
- https://www.welivesecurity.com/br/2018/10/04/10-gadgets-que-todo-hacker-etico-precisa-ter-entre-suas-ferramentas/
- https://github.com/Tinkerforge/hardware-hacking
- https://www.youtube.com/watch?v=GI9eWmk54ro

# Practice

https://www.linkedin.com/in/joas-antonio-dos-santos

# BadUSBs

- https://www.endpointprotector.com/solutions/badusb-protection
- https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/what-you-need-to-know-about-badusb
- https://www.csoonline.com/article/3087484/say-hello-to-badusb-20-usb-man-in-the-middle-attack-proof-of-concept.html
- https://github.com/armoured-ape/BadUSB-Detection
- https://github.com/caioau/badUSB-Targeting-Android
- https://opensource.srlabs.de/projects/badusb
- https://www.yubico.com/blog/yubikey-badusb/
- https://www.youtube.com/watch?v=nuruzFqMgIw
- https://www.extremetech.com/extreme/191467-badusb-returns-hackers-publish-code-that-could-infect-millions-of-usb-devices
- https://plugable.com/blogs/news/what-badusb-is-and-isnt
- https://www.youtube.com/watch?v=Ba9xMUV6wqQ
- https://www.zdnet.com/article/badusb-big-bad-usb-security-problems-ahead/
- https://fengweiz.github.io/paper/badusbc-woot21.pdf
- https://www.digitaltrends.com/computing/security-firm-releases-proof-concept-code-badusb-malware-public/

# BadUSBs 2

- https://www.youtube.com/watch?v=4Zcf4vS0DlM
- https://www.youtube.com/watch?v=6mDspyi5ROw
- https://www.facebook.com/watch/?v=381011122361082
- https://github.com/joelsernamoreno/BadUSB-Cable
- https://hacker-gadgets.com/product/evil-crow-cable-badusb/
- https://hackaday.com/tag/badusb/
- https://mg.lol/blog/badusb-cables/
- https://www.manageengine.com/device-control/badusb.html
- https://www.manageengine.com/data-security/security-threats/bad-usb.html
- https://www.bleepingcomputer.com/news/security/usbharpoon-is-a-badusb-attack-with-a-twist/

# BadUSBs 3

- https://medium.com/@ricardoiorio/vulnerabilidade-bad-usb-com-arduino-b893cceb7872
- https://nakedsecurity.sophos.com/pt/2014/08/02/badusb-what-if-you-could-never-trust-a-usb-device-again/
- https://www.youtube.com/watch?v=57J59AactV8
- https://www.youtube.com/watch?v=Utq4C9S3-uI
- https://null-byte.wonderhowto.com/how-to/make-your-own-bad-usb-0165419/
- https://www.kaspersky.com/blog/weaponized-usb-devices/26495/
- https://kryptus.com/vulnerabilidade-no-usb-badusb/

# HAK5

- https://hak5.org/
- https://hackaday.com/tag/hak5/
- https://www.youtube.com/watch?v=kqaIL_XJjSI
- https://www.youtube.com/watch?v=lAtvGksBOiw
- https://www.youtube.com/watch?v=rP1IMdE3C74
- https://aware7.de/en/blog/hacker-shop-buying-hacking-hardware/
- https://www.youtube.com/watch?v=WR5ve7cQEpY
- https://www.youtube.com/watch?v=CcnCbxoUWps
- https://www.youtube.com/watch?v=Fk1Bpy5ccPU
- https://www.youtube.com/watch?v=nmOTSd7fYdY
- https://www.youtube.com/watch?v=4kX90HzA0FM
- https://www.youtube.com/watch?v=HUzd40arX3g
- https://www.youtube.com/watch?v=LqmVaf2KHYA
- https://www.youtube.com/watch?v=qsVaC6v3NoU

# Complete Playlist Hardware Hacking

- https://www.youtube.com/playlist?list=PLL8bstVVO1fCsO46wrpYvgNqXTcDIxy4P
- Playlist of various lectures on hardware hacking at different conferences around the world

# Hardware Hacking - Courses

- http://www.grandideastudio.com/hardware-hacking-training/
- https://advancedsecurity.training/training/live-hardware-intro
- https://niccs.cisa.gov/training/search/tactical-network-solutions-llc/hardware-hacking-workshop-online
- https://www.educba.com/hardware-hacking/
- https://www.forensicinstitute.nl/training-and-expertise/training-and-courses/hardware-hacking-en-reverse-engineering
- https://www.hardware-hacking.co.uk/
- https://acaditi.com.br/curso-hardware-hacking/
- https://uniciv.com.br/cursos/ead-em-hardware-hacking/
- https://www.udemy.com/courses/search/?src=ukw&q=Hardware+Hacking
- https://www2.deloitte.com/nl/nl/events/risk-program/2020/hacklab-hardware-hacking.html
- https://www.juliodellaflora.com/treinamento

# Hardware Hacking - Techniques

- https://www.sparkfun.com/news/1314
- https://www.cyberark.com/resources/threat-research-blog/an-introduction-to-hardware-hacking
- https://gracefulsecurity.com/an-introduction-to-hardware-hacking/
- https://www.blackhat.com/html/webcast/04222021-hardware-hacking-party-tricks-techniques-for-exploring-manipulating-and-exploiting-embedded-systems.html
- https://resources.infosecinstitute.com/topic/top-19-tools-for-hardware-hacking-with-kali-linux/
- https://spectrum.ieee.org/three-ways-to-hack-a-printed-circuit-board

# Hardware Hacking - Repositorys

- https://github.com/koutto/hardware-hacking
- https://github.com/yadox666/The-Hackers-Hardware-Toolkit
- https://github.com/koutto/hardware-hacking/blob/master/Hardware-Hacking-Experiments-Jeremy-Brun-Nouvion-2020.pdf
- https://github.com/koutto/hardware-hacking/blob/master/README.md
- https://github.com/croissant-powered/hardware-hacking
- https://github.com/AcadiTi/Hardware-Hacking
- https://github.com/maldroid/hardware-hacking
- https://github.com/BusesCanFly/HardwareHackingForTheMasses
- https://github.com/htruong/hackable-consumer-hardware

# Hardware Hacking - Conferences

- https://hardwear.io/
- https://www.helpnetsecurity.com/event/hardware-hacking-virtual-conference-2020/
- https://media.defcon.org/DEF%20CON%2027/DEF%20CON%2027%20presentations/DEFCON-27-Philippe-Laulheret-Introduction-to-Hardware-Hacking-Extended-Version.pdf
- https://hackatevent.org/
- https://info.clarityexperiences.com/ioxthardwarehacking/session-mike-dow
- https://blackhat.com/
- https://redteamvillage.io/
- https://texascyber.com/

# Hardware Hacking - Laboratory

- https://hardwarehacklab.io/
- https://labs.bishopfox.com/tech-blog/how-to-set-up-your-hardware-lab
- https://www.fracturelabs.com/posts/2020/hardware-hacking-lab-physical-tools/
- https://www.youtube.com/watch?v=A0NLoMr9tHQ
- https://advancedsecurity.training/training/live-hardware-lab
- https://securityboulevard.com/2019/01/hardware-hacking-101-lesson-1-beauty-your-home-lab-and-basic-electronics/
- https://conference.hitb.org/hitb-lockdown002/virtual-labs/virtual-lab-hardware-hacking/
- https://www.hackthebox.eu/

# Hardware Hacking - Twitter

- https://www.google.com/search?q=hardware+hacking+twitter
- Hardware Hacking Professional Twitters