REVERSE ENGINEERING RESEARCH - STORM

JOAS ANTONIO

DETAILS

- I made this pdf in order to bring study materials, after I saw a vacancy at Intel Corporation that focused on exploit research and development and looking for security holes ranging from processors to software
- Fiz esse pdf com o objetivo de trazer materiais de estudo, após eu ver uma vaga na empresa Intel Corporation que focava no ramo de pesquisa e desenvolvimento de exploits e procura de brechas de seguranças que vão de processadores a softwares
- https://www.linkedin.com/jobs/view/2676920372
- My LinkedIn: https://www.linkedin.com/in/joas-antonio-dos-santos

CONCEPT

MEMORY MANAGEMENT

- https://www.tutorialspoint.com/operating_system/os_memory_management.htm
- https://en.wikipedia.org/wiki/Memory_management
- https://whatis.techtarget.com/definition/memory-management
- http://www.idc-online.com/technical_references/pdfs/information_technology/Memory_Management_Concepts.pdf
- https://www.guru99.com/os-memory-management.html
- https://isaaccomputerscience.org/concepts/sys_os_memory_management
- https://www.studytonight.com/operating-system/memory-management
- https://ecomputernotes.com/fundamental/disk-operating-system/what-is-memory-management
- https://www.ifsc.usp.br/~lattice/oldlattice/mod9.1.pdf

COMPUTER ARCHITECTURE

- https://en.wikipedia.org/wiki/Computer_architecture
- https://www.coursera.org/learn/comparch
- https://www.youtube.com/watch?v=c3mPdZA-Fmc&ab_channel=OnurMutluLectures
- https://www.youtube.com/watch?v=So9SR3qpWsM&ab_channel=NesoAcademy
- https://www.youtube.com/watch?v=_I8CLQazom0&ab_channel=ComputerScience
- https://www.sciencedirect.com/topics/computer-science/computer-architecture
- https://www.educba.com/types-of-computer-architecture/
- https://www.geeksforgeeks.org/computer-organization-and-architecture-tutorials/
- https://www.britannica.com/science/computer-science/Architecture-and-organization

CPU ARCHITECTURE

- https://developer.arm.com/architectures/cpu-architecture
- https://computersciencewiki.org/index.php/Architecture_of_the_central_processing_unit_(CPU)
- https://www.tutorialspoint.com/computer_logical_organization/cpu_architecture.htm
- https://www.youtube.com/watch?v=vgPFzblBh7w&ab_channel=IntelTechnology
- https://www.youtube.com/watch?v=rglmJ6Xyj1c&ab_channel=InfoQ
- https://www.youtube.com/watch?v=yKu43bBBu8c&ab_channel=RossMcgowan
- https://www.arm.com/why-arm/architecture/cpu
- https://www.futurelearn.com/info/courses/how-computers-work/0/steps/49283
- https://uu.diva-portal.org/smash/get/diva2:1217222/FULLTEXT01.pdf
- https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/ia-introduction-basics-paper.pdf

COMPILER

- https://en.wikipedia.org/wiki/Compiler
- https://whatis.techtarget.com/definition/compiler
- https://www.geeksforgeeks.org/introduction-of-compiler-design/
- https://www.techopedia.com/definition/3912/compiler
- https://www.youtube.com/watch?v=Y1o4rc9P1FQ&ab_channel=CppCon
- https://celsokitamura.com.br/compilador/
- https://www.dca.fee.unicamp.br/~eleri/ea876/04/cap3.pdf
- https://www.dca.fee.unicamp.br/cursos/EA876/apostila/HTML/node37.html

TECHNICAL

HARDWARE HACKING

- https://drive.google.com/file/d/1wrmZ1xlJ_zeZu8PPs1p2cLVBDcN4Pi2u/view?usp=sharing
- https://www.blackhat.com/html/bh-usa-06/train-bh-us-06-jg-h.html
- https://i.blackhat.com/USA-19/Wednesday/us-19-Tsai-Infiltrating-Corporate-Intranet-Like-NSA.pdf
- https://www.blackhat.com/docs/webcast/05192016-wheres-your-host-at-notsosecure.pdf
- https://thehack.com.br/quer-aprender-hardware-hacking-este-curso-e-perfeito-para-voce/
- https://www.youtube.com/watch?v=-WeDzPGyFxs&ab_channel=CodingTech
- https://www.youtube.com/watch?v=LSQf3iuluYo&ab_channel=MakeMeHack
- https://hackaday.com/tag/hardware-hacking/
- https://www.youtube.com/watch?v=CfljW5-Dxgk&ab_channel=BlackHillsInformationSecurity

FIRMWARE HACKING

- https://blog.nvisium.com/intro-to-hardware-hacking-dumping-your-first-firmware
- https://www.youtube.com/watch?v=oY-MxtJLEos&ab_channel=MakeMeHack
- https://www.youtube.com/watch?v=j7JRosD_ua8&ab_channel=OpenTechLab
- https://www.youtube.com/watch?v=U70unElrYbs&ab_channel=HackInTheBoxSecurityConference
- https://www.iotpentestingguide.com/firmware-hacking.html
- https://hackaday.com/tag/firmware/
- https://securelist.com/hacking-microcontroller-firmware-through-a-usb/89919/
- https://blog.attify.com/tag/firmware-hacking/
- https://www.youtube.com/watch?v=OnCcTgX0Z8c&ab_channel=Hovatek
- https://www.youtube.com/watch?v=JQRst6eiQQc&ab_channel=DahuaWikiTeamDahua
- https://embeddedbits.org/reverse-engineering-router-firmware-with-binwalk/
- https://github.com/erfanoabdi/Firmware_extractor

REVERSE ENGINEERING

- https://github.com/tylerha97/awesome-reversing
- https://gitmemory.com/alphaSeclab/awesome-reverse-engineering
- https://www.youtube.com/watch?v=IkUfXfnnKH4&ab_channel=PapoBin%C3%A1rio
- https://www.blackhat.com/docs/us-15/materials/us-15-Thomas-Advanced-IC-Reverse-Engineering-Techniques-In-Depth-Analysis-Of-A-Modern-Smart-Card.pdf
- https://www.blackhat.com/presentations/win-usa-04/bh-win-04-flake.pdf
- https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-Reverse-Engineering-The-M1.pdf
- https://www.blackhat.com/presentations/bh-europe-04/bh-eu-04-dehaas/bh-eu-04-dehaas.pdf
- https://www.blackhat.com/docs/us-14/materials/us-14-Oh-Reverse-Engineering-Flash-Memory-For-Fun-And-Benefit.pdf
- https://www.blackhat.com/presentations/bh-federal-03/bh-federal-03-eagle/bh-fed-03-eagle.pdf
- https://www.blackhat.com/presentations/bh-usa-09/QUIST/BHUSA09-Quist-RevEngCrayon-SLIDES.pdf
- https://www.blackhat.com/docs/us-16/materials/us-16-Oh-The-Art-of-Reverse-Engineering-Flash-Exploits.pdf
- https://www.blackhat.com/presentations/bh-dc-07/Sabanal_Yason/Paper/bh-dc-07-Sabanal_Yason-WP.pdf
- https://www.blackhat.com/docs/us-14/materials/us-14-Oh-Reverse-Engineering-Flash-Memory-For-Fun-And-Benefit-WP.pdf

SIDE-CHANEL ATTACK

- https://en.wikipedia.org/wiki/Side-channel_attack
- https://www.sciencedirect.com/topics/computer-science/side-channel
- https://www.sciencedirect.com/topics/computer-science/side-channel-attack
- https://searchsecurity.techtarget.com/definition/side-channel-attack
- https://www.blackhat.com/docs/us-16/materials/us-16-Hornby-Side-Channel-Attacks-On-Everyday-Applications-wp.pdf
- https://www.blackhat.com/presentations/bh-europe-08/DeHaas/Presentation/bh-eu-08-dehaas.pdf
- https://www.blackhat.com/docs/asia-17/materials/asia-17-Kim-Breaking-Korea-Transit-Card-With-Side-Channel-Attack-Unauthorized-Recharging-wp.pdf
- https://i.blackhat.com/us-18/Wed-August-8/us-18-Camurati-Screaming-Channels-When-Electromagnetic-Side-Channels-Meet-Radio-Tranceivers-wp.pdf
- https://www.youtube.com/watch?v=3v5Von-oNUg&ab_channel=MITOpenCourseWare
- https://www.youtube.com/watch?v=77oaUrRBjqw&ab_channel=RedHatCommunity
- https://www.usenix.org/conference/usenixsecurity20/presentation/luo
- https://www.usenix.org/conference/usenixsecurity18/presentation/dong
- https://www.youtube.com/watch?v=hiCOWW34eXc&ab_channel=USENIX
- https://www.youtube.com/watch?v=oRn-5giAQnk&ab_channel=MicrosoftResearch

PROGRAMMING LANGUAGE

- https://www.learnpython.org/
- https://www.coursera.org/courses?query=python
- https://medium.com/swlh/5-free-python-courses-for-beginners-to-learn-online-e1ca90687caf
- https://www.udemy.com/topic/python/free/
- https://www.pluralsight.com/courses/c-programming-language-in-action
- https://www.youtube.com/watch?v=KJgsSFOSQv0&ab_channel=freeCodeCamp.org
- https://www.youtube.com/watch?v=Bz4MxDeEM6k&ab_channel=CalebCurry
- https://www.udemy.com/topic/c-programming/
- https://www.edx.org/learn/c-programming
- https://medium.com/javarevisited/9-free-c-programming-courses-for-beginners-2486dff74065
- https://www.douglashollis.com/best-assembly-language-course-training-class-tutorial-certification-online/
- https://www.udemy.com/topic/assembly-language/
- https://siit.co/courses/assembly-language-course-and-certification/989

TRANSIENT EXECUTION CPU VULNERABILITY

- https://en.wikipedia.org/wiki/Transient_execution_CPU_vulnerability
- https://handwiki.org/wiki/Transient_execution_CPU_vulnerability
- https://gruss.cc/files/habil.pdf
- https://zims-en.kiwix.campusafrica.gos.orange.com/wikipedia_en_all_nopic/A/Transient_execution_CPU_vulnerabilities
- https://foreshadowattack.eu/foreshadow.pdf
- https://www.vusec.net/projects/blindside/
- https://www.kevinloughlin.org/dolma.pdf
- https://cipher.com/blog/a-complete-guide-to-the-phases-of-penetration-testing/
- https://securityaffairs.co/wordpress/78026/hacking/new-spectre-meltdown-attacks.html
- https://arxiv.org/pdf/1905.05725.pdf
- https://www.youtube.com/watch?v=NCVHSlmLgO8&ab_channel=IEEESymposiumonSecurityandPrivacy
- https://cobalt.io/blog/a-pentesters-guide-to-code-injection
- http://kth.diva-portal.org/smash/get/diva2:1472577/FULLTEXT01.pdf
- http://iacoma.cs.uiuc.edu/iacoma-papers/micro19_2.pdf
- https://arxiv.org/pdf/2005.13435.pdf
- https://www.researchgate.net/figure/High-level-overview-of-a-transient-execution-attack-in-5-phases-1-prepare_fig2_328938946
- https://transient.fail/
- https://lviattack.eu/
- https://www.usenix.org/conference/usenixsecurity19/presentation/canella

TRANSIENT EXECUTION CPU VULNERABILITY

- https://en.wikipedia.org/wiki/Transient_execution_CPU_vulnerability
- https://handwiki.org/wiki/Transient_execution_CPU_vulnerability
- https://gruss.cc/files/habil.pdf
- https://zims-en.kiwix.campusafrica.gos.orange.com/wikipedia_en_all_nopic/A/Transient_execution_CPU_vulnerabilities
- https://foreshadowattack.eu/foreshadow.pdf
- https://www.vusec.net/projects/blindside/
- https://www.kevinloughlin.org/dolma.pdf
- https://cipher.com/blog/a-complete-guide-to-the-phases-of-penetration-testing/
- https://securityaffairs.co/wordpress/78026/hacking/new-spectre-meltdown-attacks.html
- https://arxiv.org/pdf/1905.05725.pdf
- https://www.youtube.com/watch?v=NCVHSlmLgO8&ab_channel=IEEESymposiumonSecurityandPrivacy
- https://cobalt.io/blog/a-pentesters-guide-to-code-injection
- http://kth.diva-portal.org/smash/get/diva2:1472577/FULLTEXT01.pdf
- http://iacoma.cs.uiuc.edu/iacoma-papers/micro19_2.pdf
- https://arxiv.org/pdf/2005.13435.pdf
- https://www.researchgate.net/figure/High-level-overview-of-a-transient-execution-attack-in-5-phases-1-prepare_fig2_328938946
- https://transient.fail/
- https://lviattack.eu/
- https://www.usenix.org/conference/usenixsecurity19/presentation/canella

HARDWARE (RTL) DESIGN

- https://link.springer.com/chapter/10.1007/978-3-319-16214-0_5
- https://www.sciencedirect.com/topics/computer-science/register-transfer-level
- https://semiengineering.com/knowledge_centers/eda-design/definitions/register-transfer-level/
- https://en.wikipedia.org/wiki/Register-transfer_level
- https://pt.wikipedia.org/wiki/Register_transfer_level
- https://www.intel.com.br/content/www/br/pt/software/programmable/overview.html
- https://www.intel.com.br/content/www/br/pt/software/programmable/quartus-prime/hls-compiler.html
- https://jobs.intel.com/ShowJob/Id/2867857/FPGA-RTL-Design-Engineer
- https://jobs.intel.com/page/show/connectivity-jobs-rtl-integration

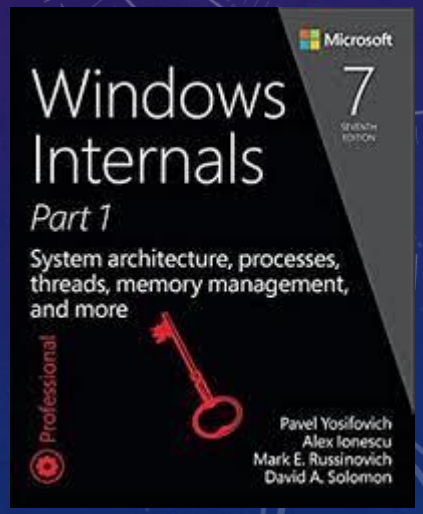
BINARY EXPLOITATION

- https://github.com/HenryHoggard/awesome-arm-exploitation
- https://www.youtube.com/watch?v=tMN5N5oid2c&ab_channel=JohnHammond
- https://www.youtube.com/watch?v=i5-cWI_HV8o&ab_channel=JohnHammond
- https://www.youtube.com/watch?v=gxU3e7GbC-M&ab_channel=SourceMeetsSink
- https://www.youtube.com/watch?v=WnqOhgI_8wA&ab_channel=PwnFunction
- https://trailofbits.github.io/ctf/exploits/binary1.html
- https://www.youtube.com/watch?v=72GShSHsRZI&ab_channel=PinkDraconian
- https://www.youtube.com/watch?v=akCce7vSSfw&ab_channel=LiveOverflow
- https://www.youtube.com/watch?v=Hp_YVg5QFEw&ab_channel=AmritaInCTFJunior
- https://github.com/r0hi7/BinExp

SOFTWARE REVERSE ENGINEERING

- https://eforensicsmag.com/course/software-reverse-engineering-techniques-level-1/#:~:text=Software%20Reverse%20Engineering%20Techniques%20is,program%20or%20even%20debug%20it.
- https://en.wikipedia.org/wiki/Reverse_engineering
- https://www.apriorit.com/dev-blog/366-software-reverse-engineering-tools
- https://www.researchgate.net/publication/259563782_An_introduction_to_software_reverse_engineering
- https://searchsoftwarequality.techtarget.com/definition/reverse-engineering
- https://securityaffairs.co/wordpress/46606/hacking/software-reverse-engineering-process-basics.html
- https://www.quora.com/What-techniques-and-tools-are-existed-for-software-reverse-engineering
- https://link.springer.com/chapter/10.1007/978-3-642-04117-4_31
- https://www.informit.com/articles/article.aspx?p=353553&seqNum=5
- https://astromachineworks.com/what-is-reverse-engineering/
- https://ethics.csc.ncsu.edu/intellectual/reverse/study.php

CERTIFICATIONS



Pavel