References used for the project

1. Bootstrapping

1.1. Trusted Boot

- *S. Zimmo, A. Refaey and A. Shami, "Trusted Boot for Embedded Systems Using Hypothesis Testing Benchmark," 2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), London, ON, Canada, 2020, pp. 1-2, doi: 10.1109/CCECE47787.2020.9255703*

- *Khalid, O., Rolfes, C., & Ibing, A. (2013, June). On implementing trusted boot for embedded systems. 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST). http://dx.doi.org/10.1109/hst.2013.6581569*

- Landry, J. (2019, July 22). *What is the hardware root of trust?* Dell. https://www.dell.com/en-us/blog/hardware-root-trust/

- *5 elements to secure embedded system – part #2 root-of-trust (rot)*. (2021, June 24). Beningo Embedded Group. https://www.beningo.com/5-elements-to-secure-embedded-system-part-2-root-of-trust-rot/

1.2. Secure Boot

- *R.V., R., & A., K. (2018, March). Secure boot of Embedded Applications - A Review. 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA). http://dx.doi.org/10.1109/iceca.2018.8474730*

- *Profentzas, C., Gunes, M., Nikolakopoulos, Y., Landsiedel, O., & Almgren, M. (2019, May). Performance of secure boot in embedded systems. 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS). http://dx.doi.org/10.1109/dcoss.2019.00054*

- *EmbeddedWala. (2022, August 30). Boot sequence of ARM based MCU. Embedded Wala. https://embeddedwala.com/Blogs/embeddedsystem/bootsequenceofarmbasedmcu*

- Secure Boot in SimpleLink CC13x2/CC2x2 Wireless MCUs. Texas Instruments. https://www.ti.com/lit/an/swra651/swra651.pdf?ts=1676995431935&ref_url=https%253A%252F%252Fwww.google.com%252F

- *5 elements to secure embedded system – part #2 root-of-trust (rot)*. (2021, June 24). Beningo Embedded Group. https://www.beningo.com/5-elements-to-secure-embedded-system-part-2-root-of-trust-rot/

- *5 elements to secure embedded systems – part #3 secure boot*. (2021, July 8). Beningo Embedded Group. https://www.beningo.com/5-elements-to-secure-embedded-systems-part-3-secure-boot/

- *Tips and tricks – jumping from the bootloader to the application code cleanly*. (2017, August 24). Beningo Embedded Group. https://www.beningo.com/tips-and-tricks-jumping-from-the-bootloader-to-the-application-code-cleanly/

2. Security

A lot of explanation can be found about MPU, HSM, and Cryptography in this document:

- Overview of Secure Boot and Secure Firmware Update solution on Arm TrustZone STM32 microcontrollers. STMicroelectronics. https://www.st.com/resource/en/application_note/an5156-introduction-to-stm32-microcontrollers-security-stmicroelectronics.pdf
- A Survey of Information Security Implementations for Embedded Systems. WNDRVR.

- Ltd., A. (n.d.). *TrustZone for cortex-m – arm®*. Arm | The Architecture for the Digital World. Retrieved February 21, 2023, from https://www.arm.com/technologies/trustzone-for-cortex-m

- Joshi, P. (2022, August 5). *Common Attacks on Embedded Systems and its prevention*. Rsk-Cyber-Security. https://rsk-cyber-security.com/blog/common-attacks-on-embedded-systems-and-how-to-prevent-them/

- Arm Platform Security Architecture Trusted Boot and Firmware Update 1.0. Arm. https://developer.arm.com/-/media/Arm%20Developer%20Community/PDF/PSA/DEN0072-PSA_TBFU_1.1-BETA0.pdf?revision=3ce2513a-ae0f-4b43-96a0-851ed67a640b

3. **Cryptography fundamentals**

- Applied Cryptography in Embedded systems. University of VAASA. https://osuva.uwasa.fi/bitstream/handle/10024/6687/osuva_5564.pdf

- Ram, V. (2022, August 3). How to implement a sample hash table in C/C++. *DigitalOcean*. https://www.digitalocean.com/community/tutorials/hash-table-in-c-plus-plus

4. **Measuring time**

- Moreno, C., & Fischmeister, S. (2017). Accurate measurement of small execution times—getting around measurement errors. *IEEE Embedded Systems Letters*, *9*(1), 17–20. https://doi.org/10.1109/les.2017.2654160

- Karl, O., & Rabi, M. (2018). Hardware Performance Counters for Embedded Software Anomaly Detection. https://DOI 10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00101