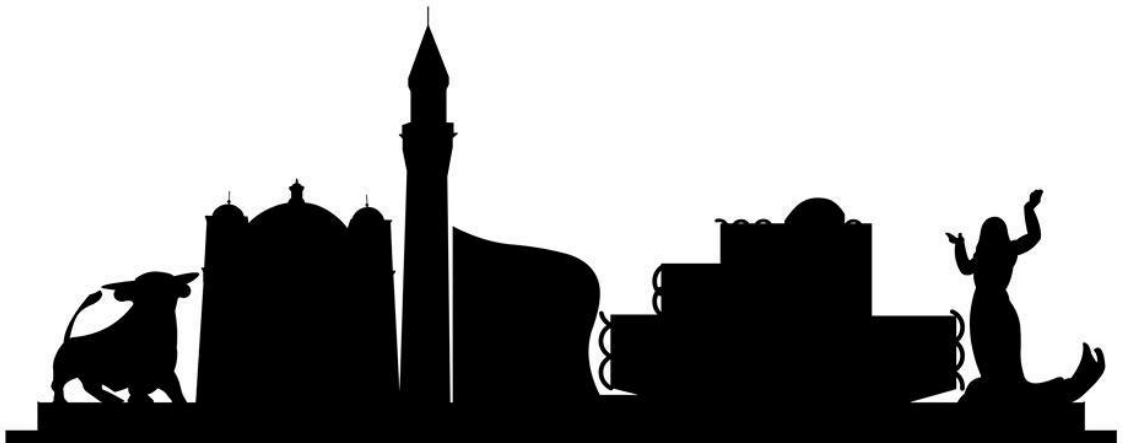
BREAKING BOOTLOADERS ON THE CHEAP

PRESENTED BY:

QAIS TEMEIZA

@qaistemeiza

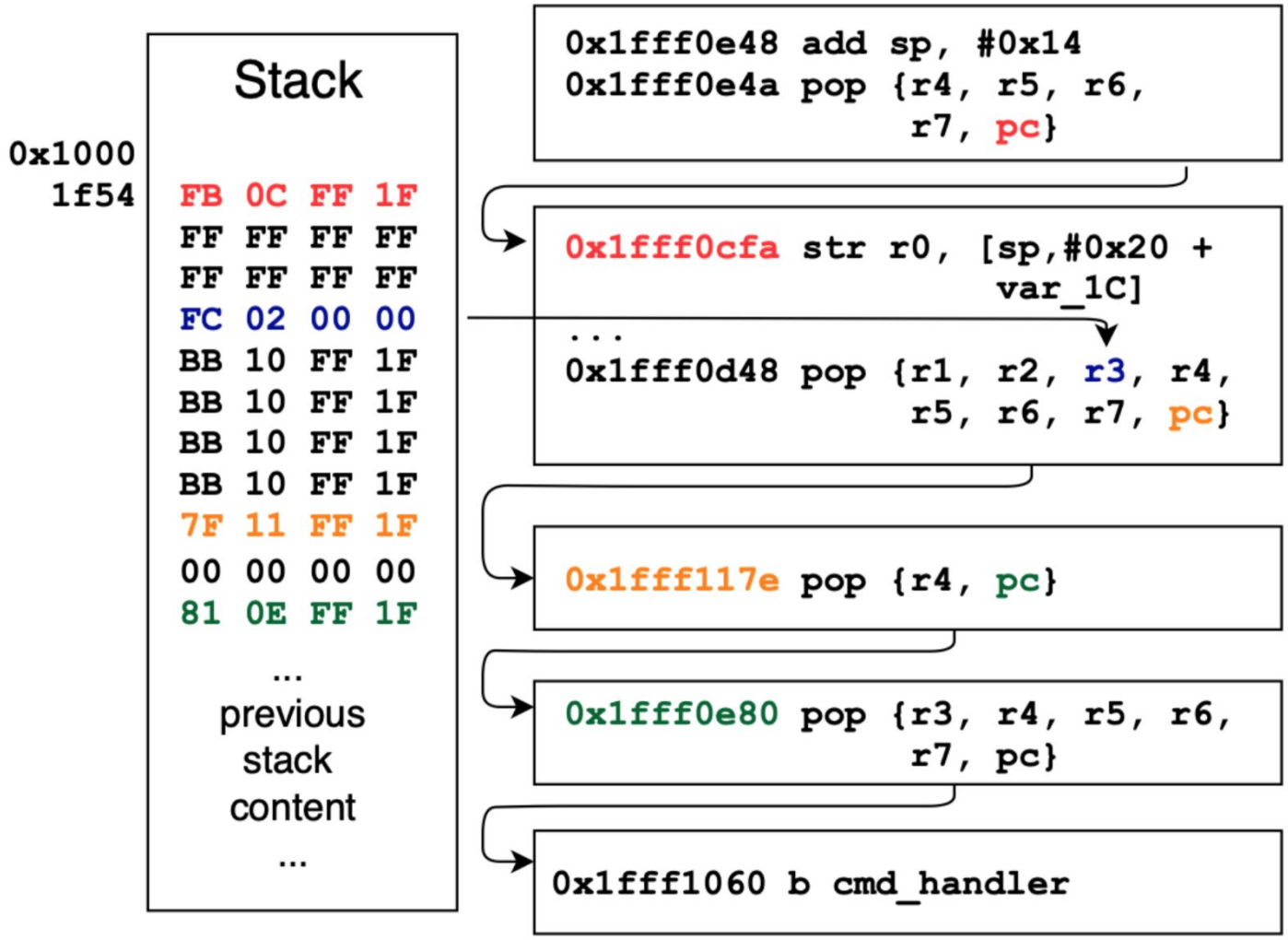


Introduction

LPC1343 Vulnerabilities

- Critical vulnerability in the LPC1343 write to RAM command, which lead to breaking CRP1
- Partial overwrite attack
- Some parts of the bootloader memory is not protected in CRP1

Write to RAM Command Vulnerability

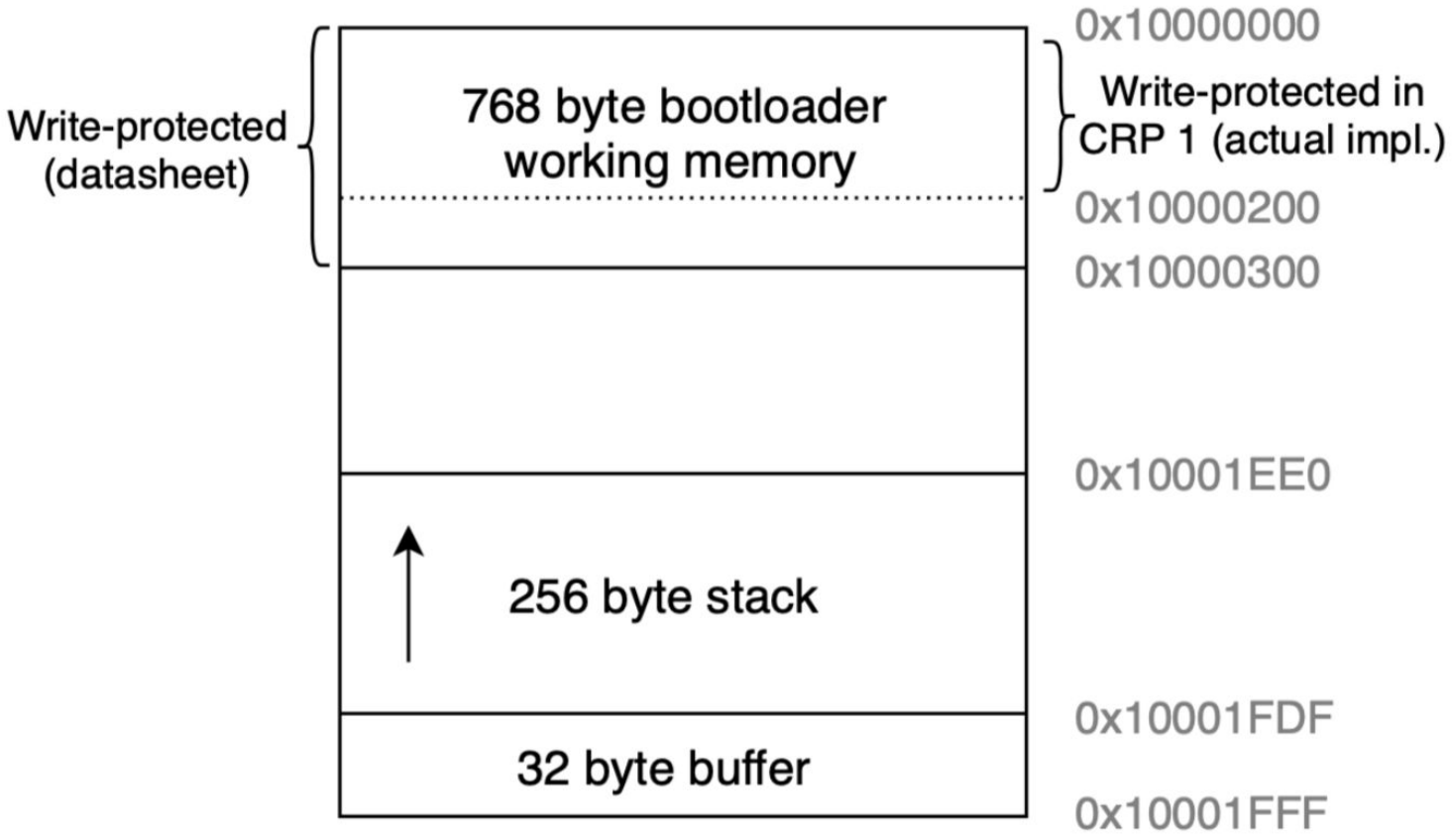


Source: https://tches.iacr.org/index.php/TCHES/article/view/8727/8327

Partial Overwrite Vulnerability

- The attacker copies his dumper to one of the sectors
- When resetting the device, the dumper will get called and start dumping all other sectors
- A second Identical device will be used to overwrite a different sector, in order to get the data of the previously overwritten sector

Bootloader Memory Protection



Source: https://tches.iacr.org/index.php/TCHES/article/view/8727/8327

Summary

References

- https://tches.iacr.org/index.php/TCHES/article/view/8727
- https://i.blackhat.com/eu-19/Thursday/eu-19-Temeiza-Breaking-Bootloaders-On-The-Cheap-2.pdf
- https://github.com/qais744/LPC-ROP
- https://github.com/janvdherrewegen/bootl-attacks