Table of contents

1. The problem
   1. Control-flow attacks
      1. ROP
      2. Instruction skipping
      3. Direct memory attacks
2. The requirements
3. Control-flow
4. Related work
   1. CFI protection
      1. Software
      2. Hardware
   2. CFI attestation
      1. Software
      2. Hardware
   3. Hardware/software binding
5. Project solution
   1. Hardware requirements
      1. ARM Architecture
         1. Introduction
         2. TrustZone
         3. M vs A Trustzone
      2. FPGA
   2. Static Attestation
   3. Dynamic Attestation
      1. Building CFG (Needs further research)
      2. Run-time tracing of control-flow
      3. Storage
         1. Contents
            1. Storage of CFG
            2. Current running programs
            3. External data
            4. Internal data
            5. Previous hash
         2. Encryption (Needs further research)
   4. Provisioning (Needs further research)
6. Further work
7. Conclusion