Table of contents

1. Introduction
   1. Control flow **1 day**
   2. Attacks on control flow **1 day**
      1. ROP
      2. Instruction skipping
      3. Direct memory attacks
   3. Problem description **0.3 day**
   4. Project objectives **0.3 day**
   5. Project structure **0.3 day**
2. Control Flow Integrity (CFI)
   1. Control-flow graph construction **1 day**
      1. Basic blocks
   2. Prevention **2 days**
      1. Software
      2. Hardware
   3. Detection **2 days**
      1. Software
      2. Hardware
   4. Attestation **2 day**
      1. Software
      2. Hardware
3. Associated background **2 days**
   1. Static Attestation
   2. Secure Software Execution – other approaches (previous lit review e.g. binding)
   3. Arm TrustZone
4. Comparison of solutions **1 day**
5. Theoretical solution **??**
   1. Static Attestation
   2. 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)
   3. Provisioning (Needs further research)
6. Practical implementation **??**
7. Security analysis **1 day**
8. Conclusion/further work