Control Flow Integrity Based Security – Seminar
Draft outline of Research Paper

Section 1: Control-Flow Integrity
- Introduction
- Current Implementations

Section 2: Derivatives of the “Control-Flow Integrity: precision, Security, and Performance” paper by Nathen Burow et. al.
- Difficulties in establishing a unified metric
- Reality of Performance/Security trade-off

Section 3: Next Generation
- Eliminating the cons: recent trends
- Hardware-supported CFI
- Just in-in-time Compiled Code

Section 4: Evaluation

Section 5: Conclusion

Description:

After reading through the paper I have decided on the above outline for my research paper. I would like to note that this is not final, and especially the titles will be subject to change during my research.

The paper will be divided into different sections which I will explain below.

Section 1 will be the general introduction to the topic I would like to tackle. Giving information about CFI and its current information is necessary to give context to the other sections.

Section 2 will follow mostly the paper assigned to me in the course. Here the authors took on the challenge of establishing a unified metric of measuring the effectiveness of different CFI implementations. The methodology used is an analogy to the way graphical performance of hardware is measured in graphically intense applications such as rendering and gaming. This will be a vital part of my paper because these metrics and repercussions stay true for section 3 as well.

Section 3 will focus on the problems stated by section 1 and section 2 like for example the Performance to security trade-off and how research and future implementations are further trying to improve upon.

Section 4 will by the evaluation of the different metrics proposed on the new implementations and will try to provide a comparison between relevant implementations, old (to an extent) and new.

Section 5 will be my conclusion as well as recommendations.
References:

Most of the papers I have gathered until now are different citations used in the paper by Nathan Burow et. al. Due to the nature of his paper his citations provide many relevant references in which I am still working myself into.

This roster is of course going to be further extended while my paper is fleshed out.