PRNGs in Linux (Research Track)

1. Team members

Zane Goldhahn	p72n371
Garrett Perkins	m95m353
Ethan Fison	t85j427
John Dolph	r87f693

2. Overview

This project will focus on a deep dive into pseudorandom number generation and its implementation in the linux kernel. Relevant topics include gathering entropic data from system hardware, cryptographic algorithms (PRNGs), hardware-level PRNGs (maybe not this one, though I would expect that there's still some amount of info in the kernel), and of course, discussion on the importance of a robust RNG solution.

Optionally:

If we need more topics to cover: Microsoft has a whitepaper out on the implementation for windows, which could be worth looking into, if at least for comparison.

3. Deliverables

Primary: Paper discussing our findings on the inner workings of the Linux kernel’s random number generation.

Secondary: Presentation (slides, data structure visualizations, other diagrams, etc) and video recording.

4. Schedule

11/1: Have general outline in place for each section, begin digging through code for basic understanding of functions.

11/7: Begin filling out sections, prepare diagrams as needed. Begin working on slides/ presentation structure

11/13: Finalize sections/presentation. Prepare presentation video

5. Division of Labor

Table 1: Division of labor percent responsibility

Name	**Research**	**Documentation**	**Presentation**
Zane	25%	25%	25%
Garrett	25%	25%	25%
Ethan	25%	25%	25%
John	25%	25%	25%