Cost of Security Auditing Focus

Matthew Chambers (Michigan Technological University)
Kevin Lopez (California State University, San Bernardino)
Casey Mortensen (New Mexico Institute of Mining and Technology)

Mentor: David Kennel (DCS-1)
Instructor: Andree Jacobson (NMC)

2011 Computer System, Cluster and Networking Summer Institute

Los Alamos
NATIONAL LABORATORY
EST.1943

NSF

ISTI
INFORMATION SCIENCE & TECHNOLOGY INSTITUTE

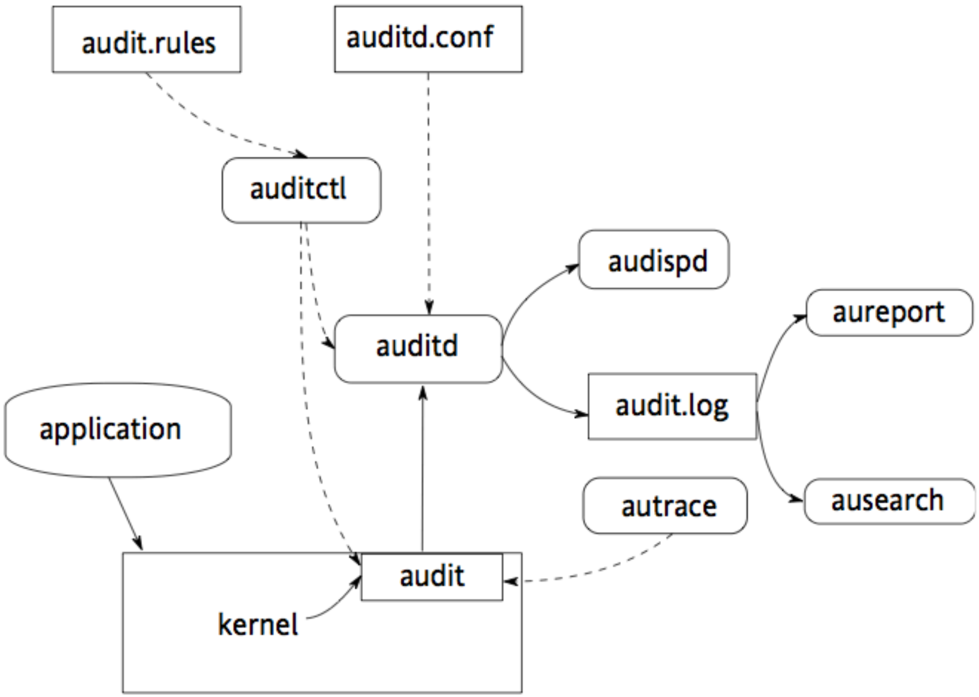
New Mexico
CONSORTIUM
NM STATE UNIVERSITY
NEW MEXICO TECH
The University of New Mexico

Introduction

- What is the audit daemon?
- What purpose does auditd serve?
- What is the cost of security?

Auditd

- Kernel level service
- Intrusion Detection System
- Does not prevent malicious activity



Novell © - http://www.novell.com/documentation/sled10/pdfdoc/audit_sp1/audit_sp1.pdf

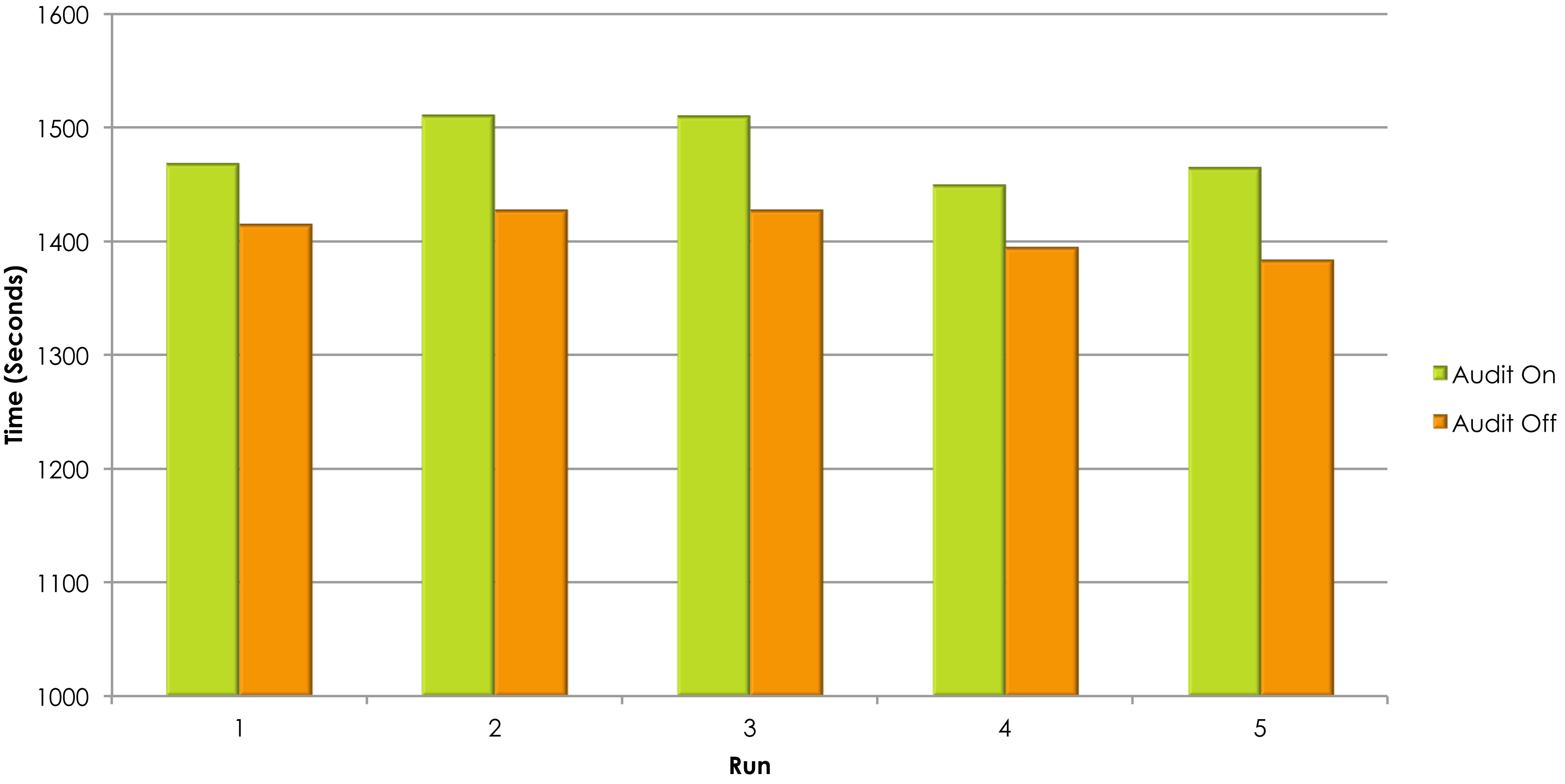
The Benefits of Auditd

- Increased security
  - Monitor file activity
  - Monitor syscall activity
- Creates detailed logs
  - User info, syscall used, timestamp, etc.
- Robust search and filter implementations
- Easy, manageable logging rotation solution

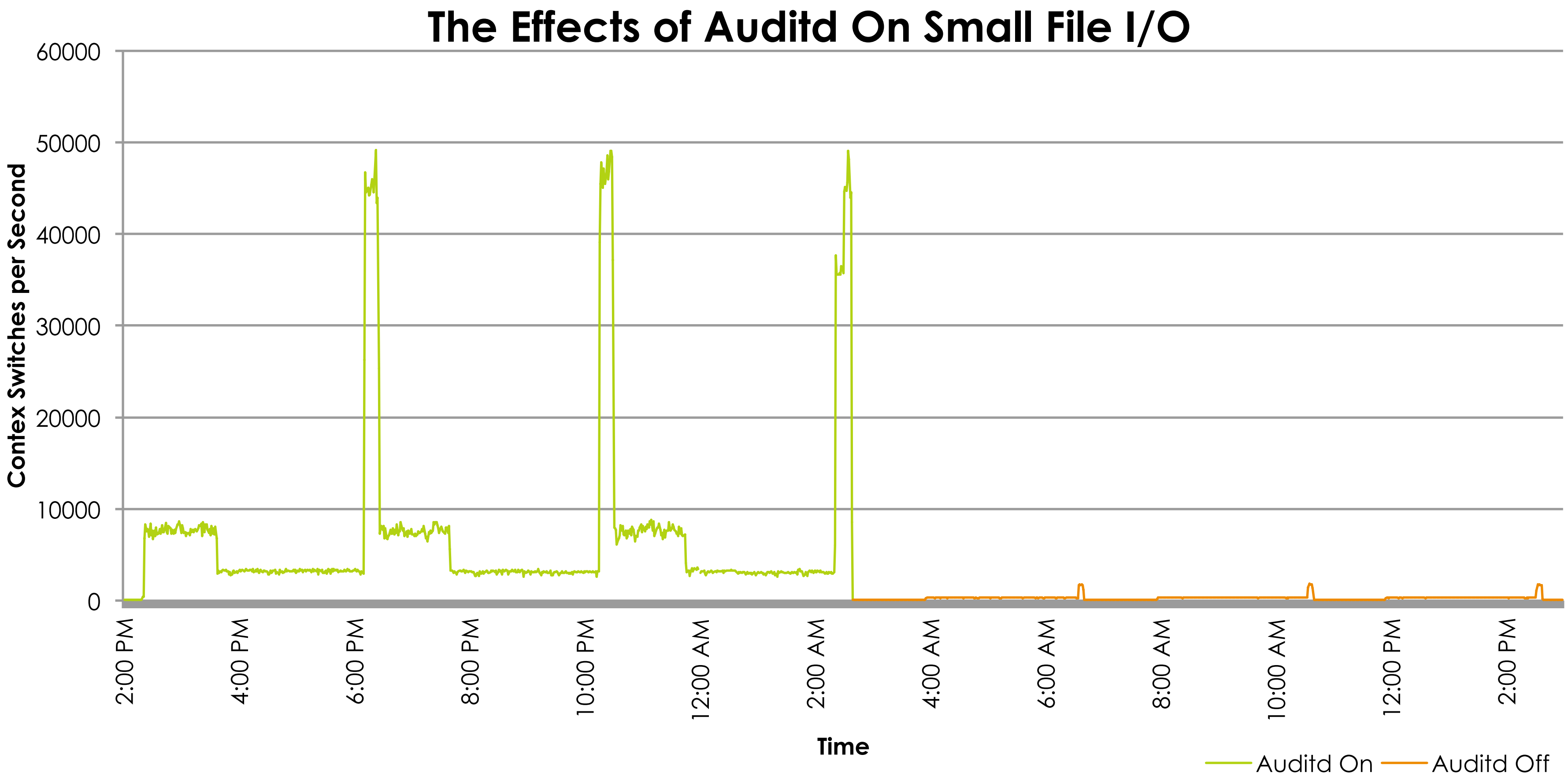
The Drawbacks of Auditd

- Performance degradation
  - CPU interrupts
  - Context Switching
  - Logging
- Only a detection system

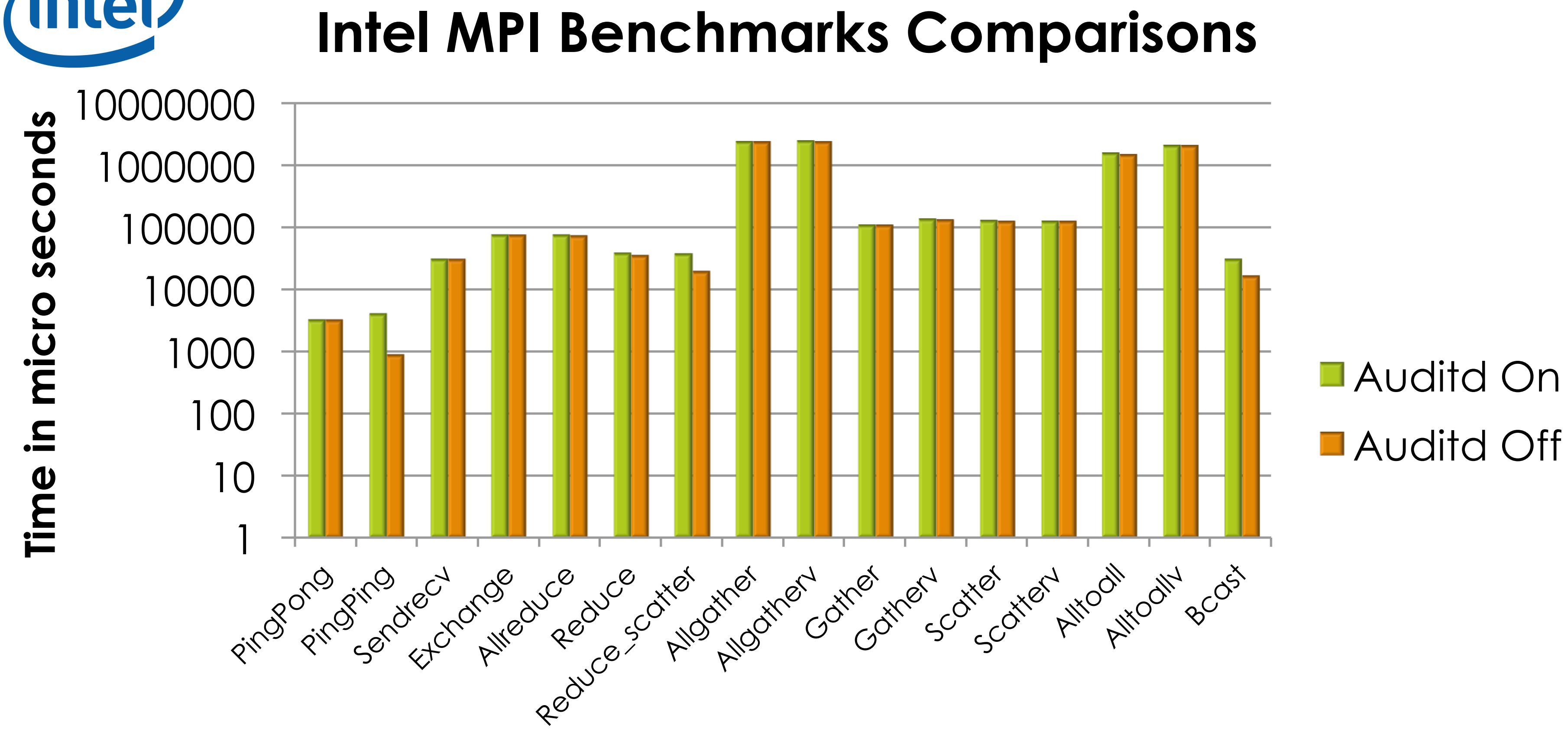
Results (Small File I/O)



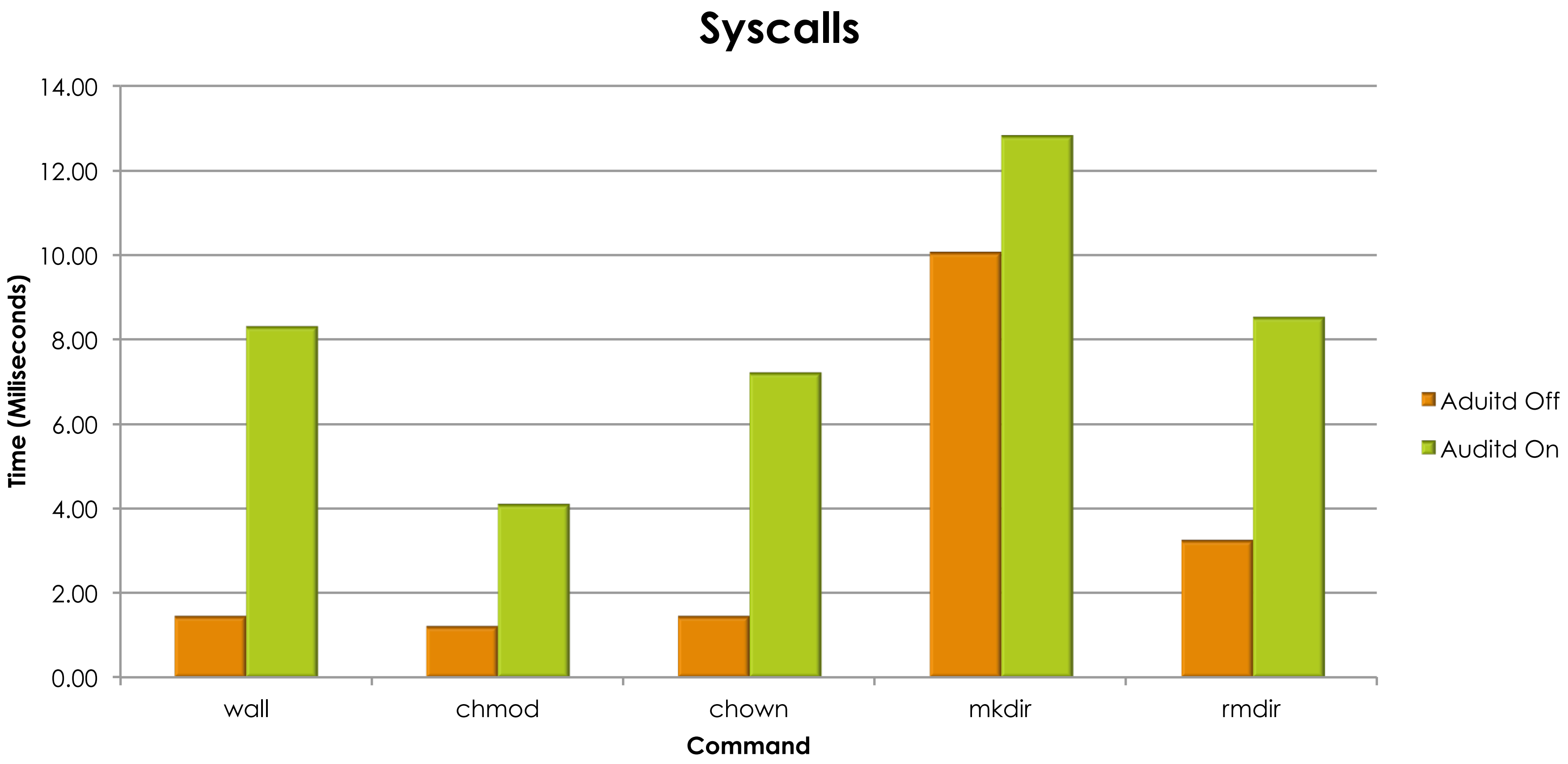
Results (Small File I/O)



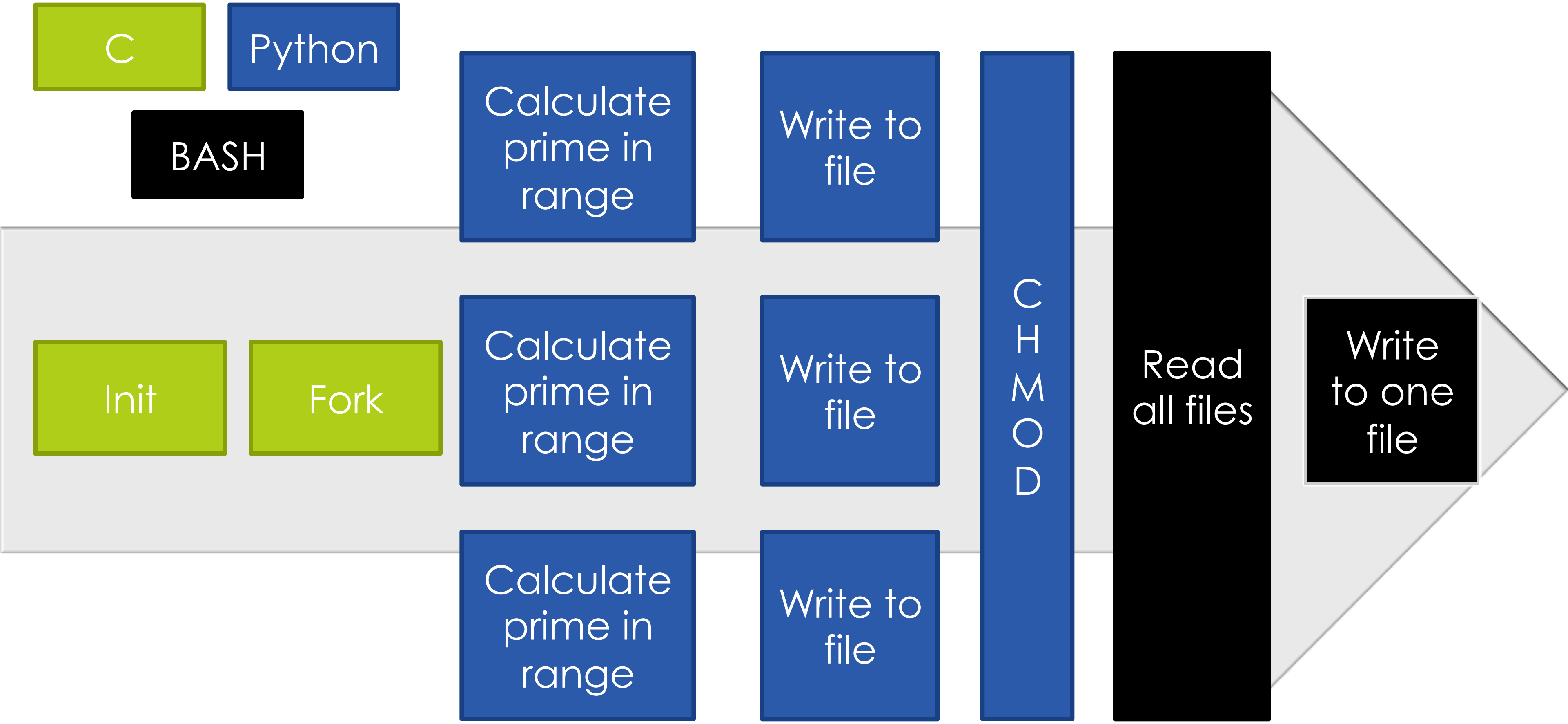
Results (Intel MPI)



Results (Syscalls)



Hybrid Benchmark



C

Python

BASH

Init

Fork

Calculate prime in range

Calculate prime in range

Calculate prime in range

Write to file

Write to file

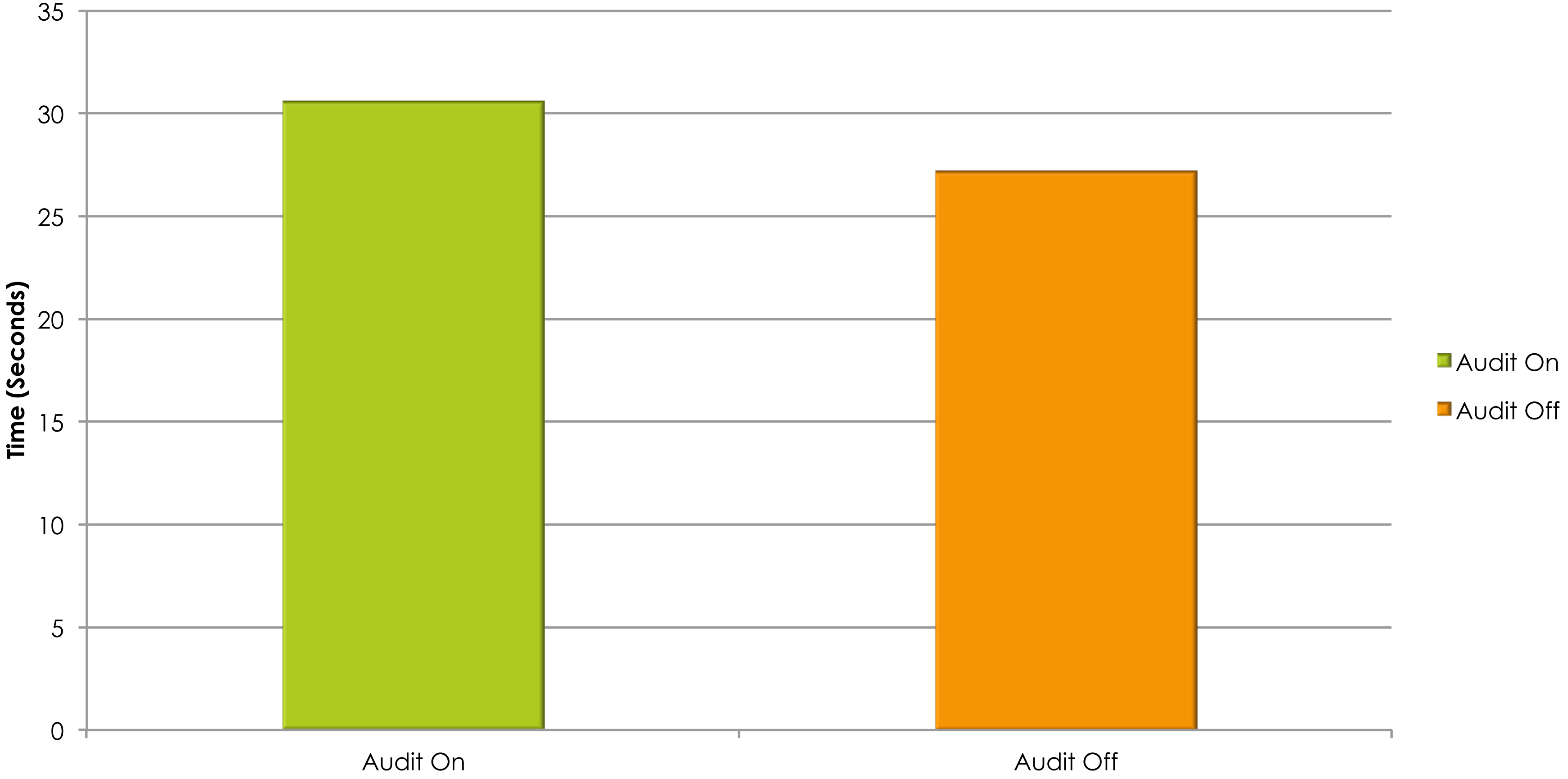
Write to file

CHMOD

Read all files

Write to one file

Results (Hybrid)



What to consider…

- Scaling
- Protection Measures (SE Linux)
- NFS vs Audit Dispatcher
- SSD and RAM performance

Conclusion

- Performance Cost
  - Non-CAPP rules
  - CAPP Rules
- Recommendation
  - Minimal day to day impact
  - Implement Auditing

Questions?