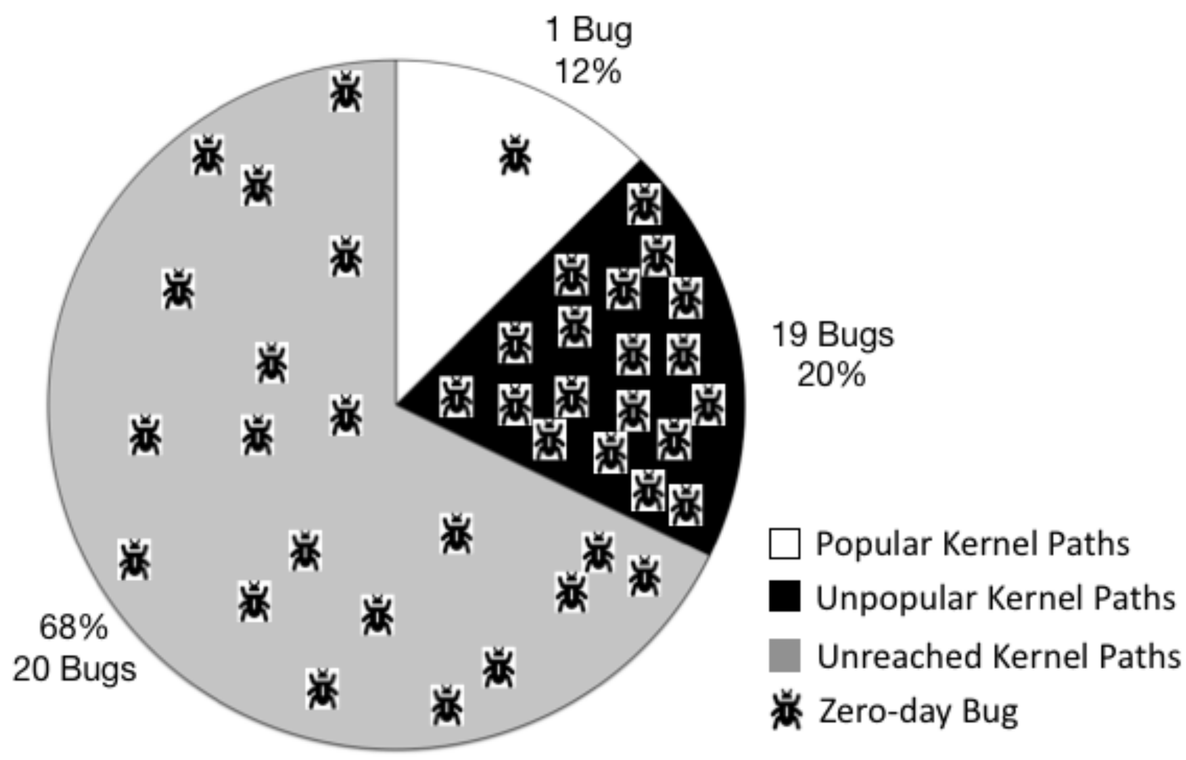
# Lind – A Secure Library OS VM

Justin Cappos, NYU Tandon School of Engineering
https://lind.poly.edu

## Lock-in-Pop Design: Only Access Popular Paths in the Kernel

**Project Goal**: Allow untrusted code to run on top of a vulnerable host OS
**Key insight**: **Popular kernel paths contain fewer bugs**




## Approach

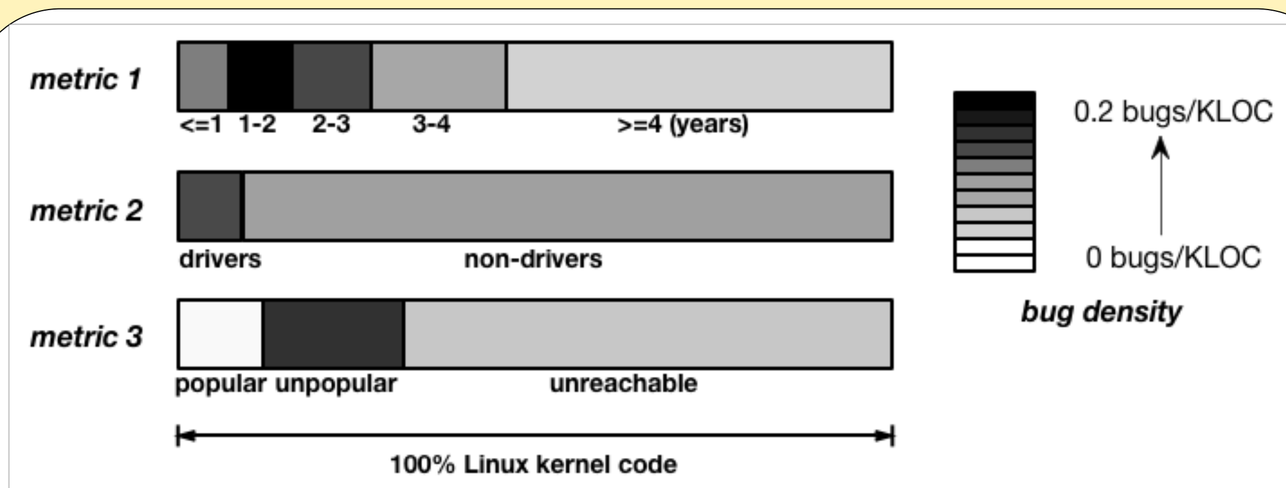
### Quantitative Security Metric

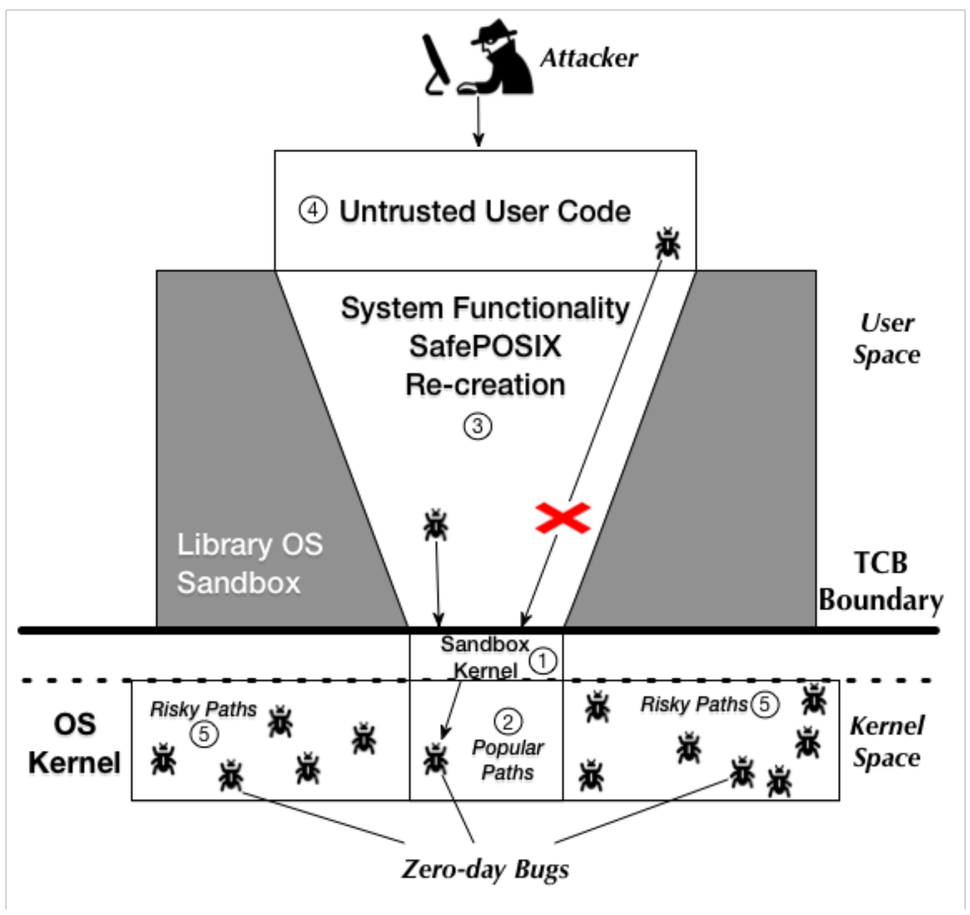
- Identify the lines of code executed in the kernel
- Analyze bug distribution in the kernel

*Popular paths metric is effective!*

### Lock-in-Pop Design

- A minimal sandbox kernel - only access popular paths
- SafePOSIX re-creation – implement complex and risky OS functionality




## Evaluation Results

| VM | Bugs Triggered |
|---|---|
| Docker | 8/35 (22.9%) |
| LXC | 12/35 (34.3%) |
| Graphene | 8/35 (22.9%) |
| Lind | 1/35 (2.9%) |

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

NYU TANDON SCHOOL OF ENGINEERING