Trustworthy Unpredictability: Creating an Unfavorable Environment for Stealthy Malware at the OS Level

Ruimin Sun, University of Florida

Motivation

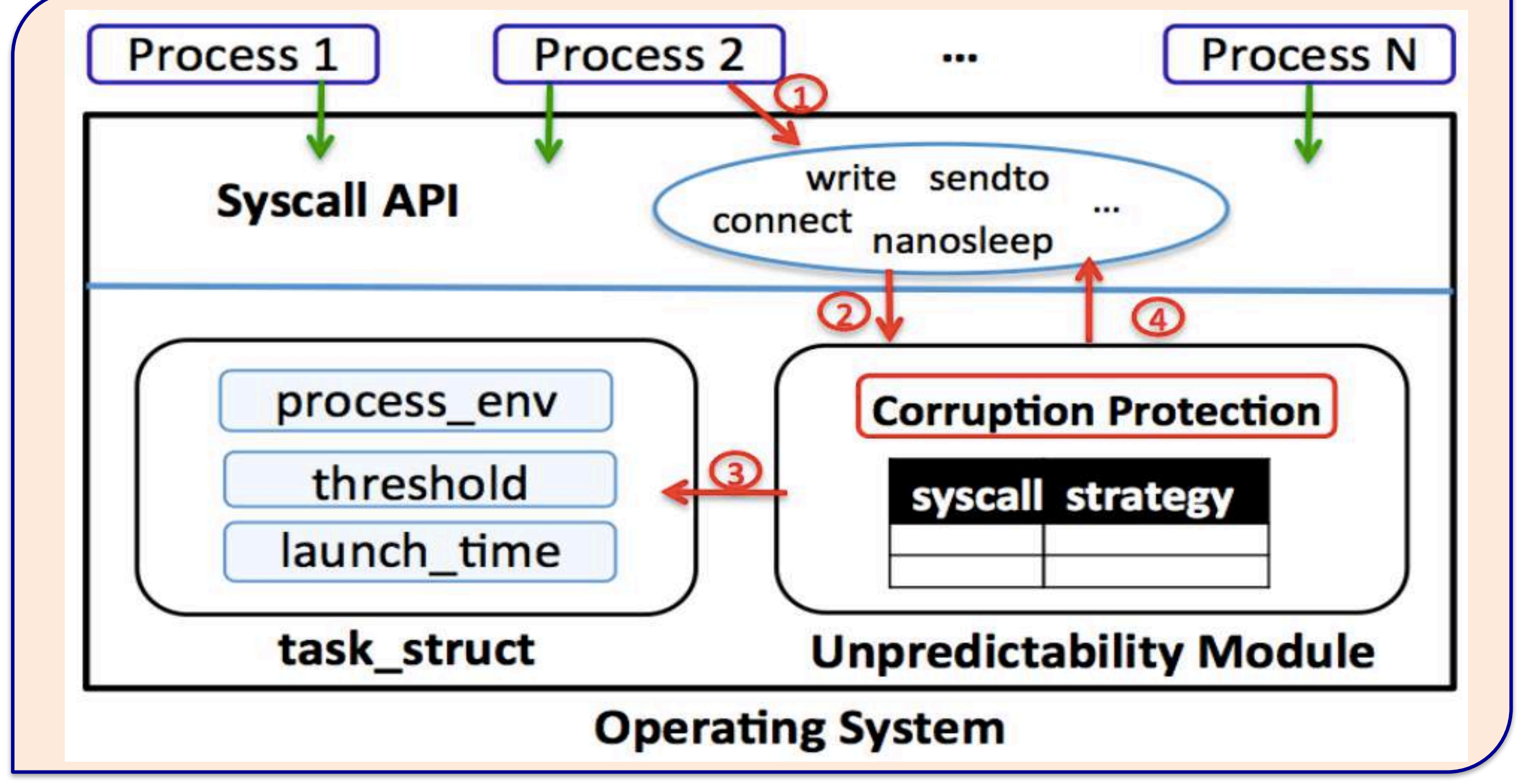
Computer systems are designed to be **predictable** for its reliability, consistency in common software development. Its **downside** is that attackers can leverage the same vulnerabilities on thousands of identical systems. What will happen if we bring some unpredictability?

Trustworthy Unpredictability

- Name: Bob   Age: 78
- Living in a retirement community in Florida.
  - * Skype with son
  - * Online games

> ➢ *Phishing email?*
> ➢ *Becoming a Bot?*

Architecture



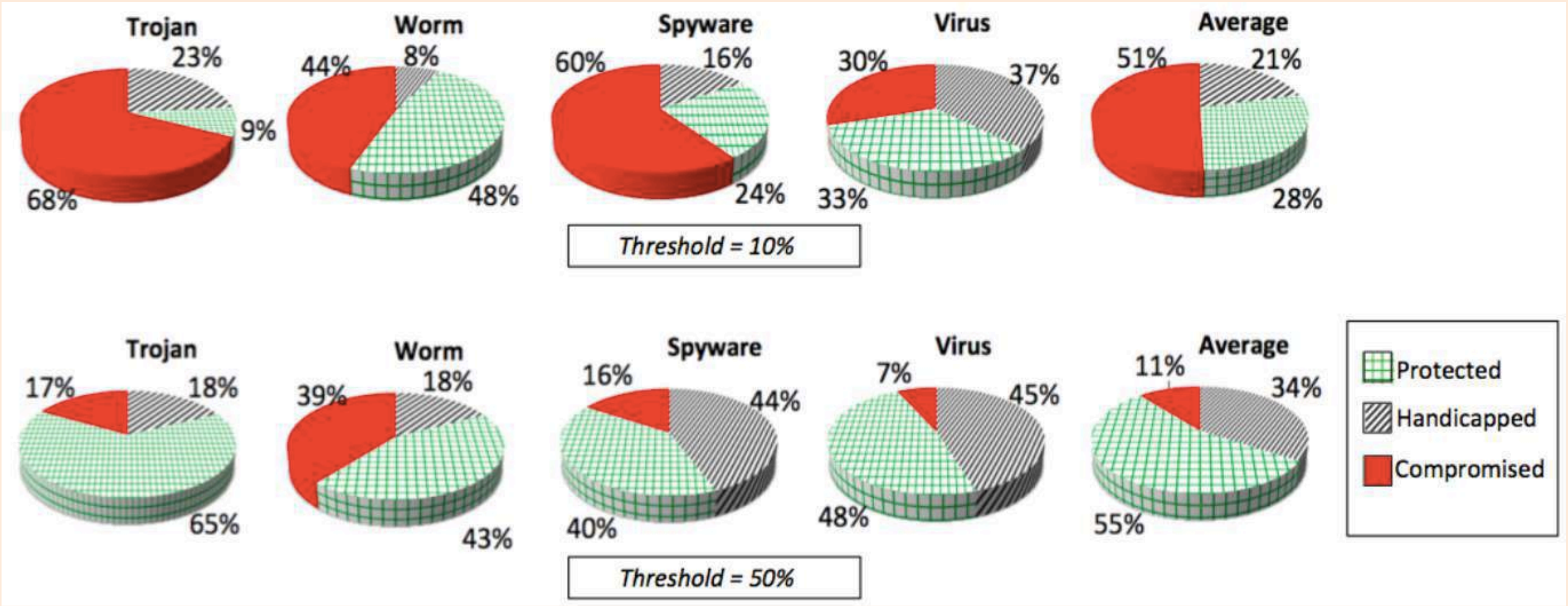
Strategies

- System call silencing
- Buffer bytes change
- System call delay
- Connection restriction
- File offset change

Syscall	Strategies
sys_write	1, 2, or 5
sys_read	1, 2, or 5
sys_lseek	1 or 5
sys_sendto	1, 2, or 5
sys_recvfrom	1, 2, or 5
sys_bind	1
sys_nanosleep	1 or 3
sys_connect	1 or 4
sys_listen	1 or 4

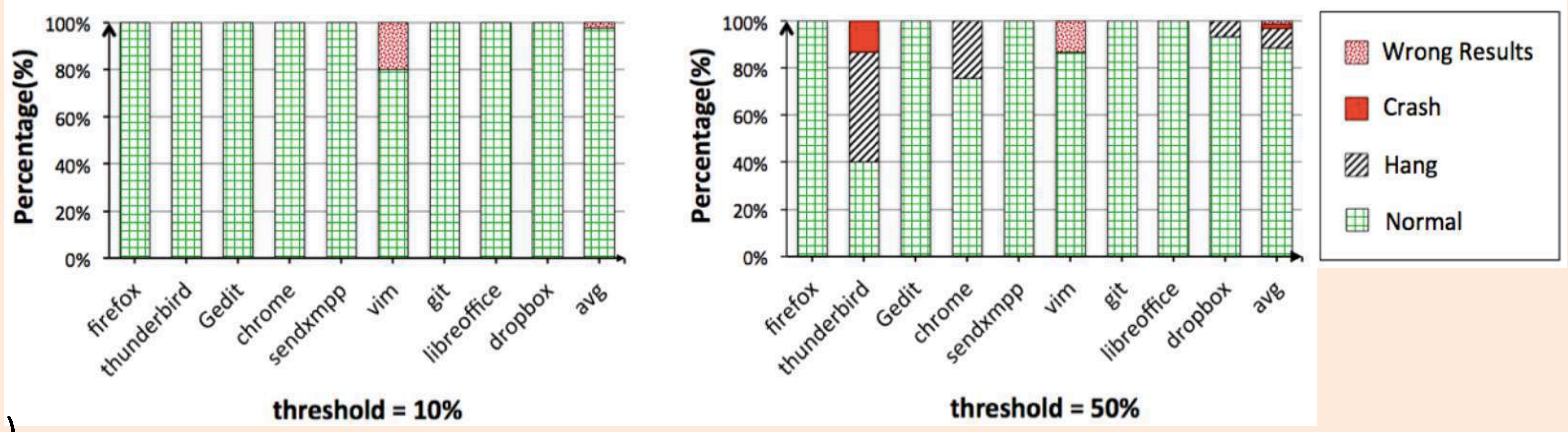
Unpredictability on Malicous and Benign Software

- Tested Unpredictability on 15 malware and 15 benign software
- With unpredictability, system is protected from malware



- Unpredictability on Malware (Trojan, Worm, Spyware and Virus)

- CPU bound software are ***resilient*** to unpredictability
- I/O bound software can tolerable unpredictability for most of the time (threshold 10%)



- Unpredictability on **I/O bound** software