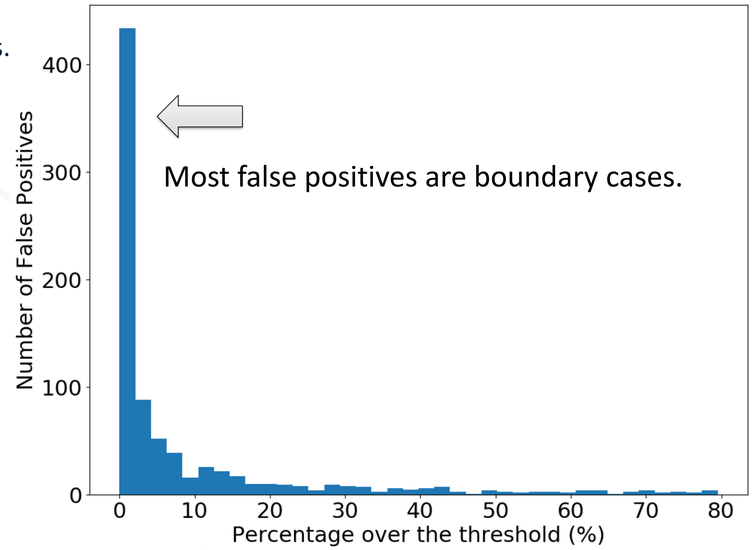
A Hybrid Approach to Security Attack Detection in Containerized Applications

Yuhang Lin (ylin34@ncsu.edu), Xiaohui Gu (xgu@ncsu.edu)

North Carolina State University

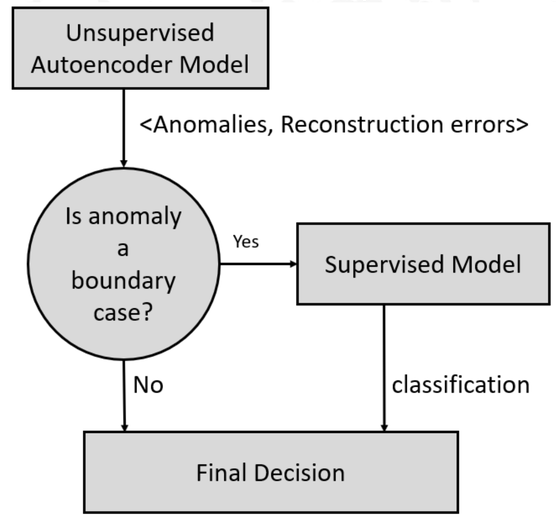
Motivation

- Containerized applications have many security vulnerabilities.
- Previous work proposes supervised and unsupervised approaches.
- However, false positives are still too high to be practical.



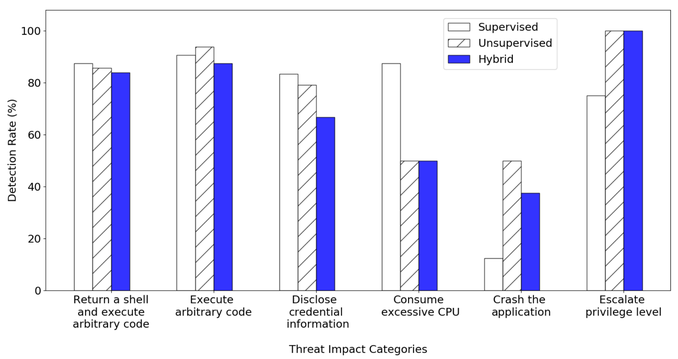
Hybrid Approach

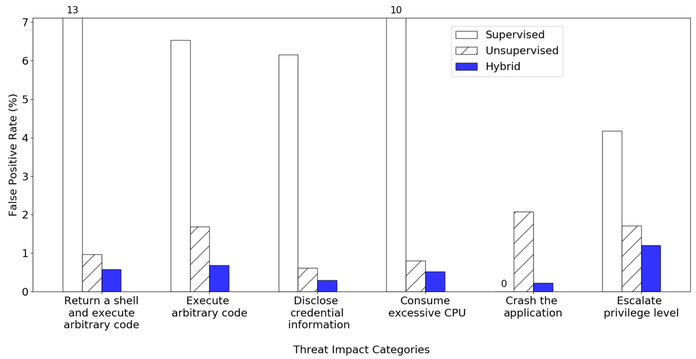
Combine supervised and unsupervised learning.

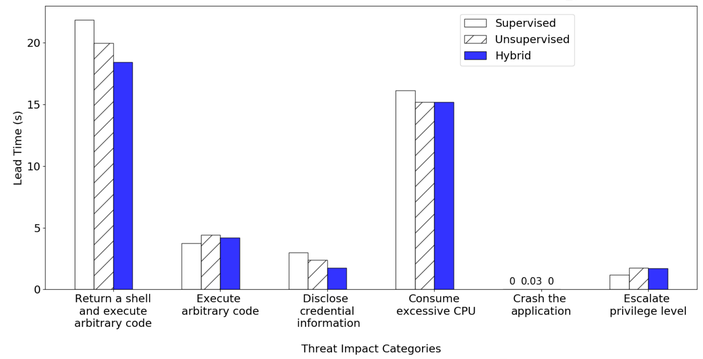


Results

- We evaluate over 33 real world vulnerabilities in 24 commonly used server applications.
- Our hybrid approach reduces false positive rate by 52.6% while only reduces detection rate by 6.4%.







8TH ANNUAL HOT TOPICS *in the* **SCIENCE OF SECURITY**
APRIL 13-15, 2021 | VIRTUAL