Ups and Downs of Cloud Computing in Open Science - Some Security Musings

Mike Stanfield
Senior Security Analyst
Center for Applied Cybersecurity Research
Indiana University

CI/CS WORKSHOP ResearchSOC | CI CoE PILOT

A quick mention of risk analysis

- Before you decide to deploy to the cloud you should think about the risk difference between on-prem and cloud
    - For most scientific applications this is probably pretty minimal
        - Availability and integrity are primary drivers - we have existing solutions for these problems
    - If you are handling restricted data, may want to give this extra thought
        - Harder to protect data outside your direct control
- Given that, I'm not going to spend time discussing risks related to sharing hardware with a potential attacker (Rowhammer, Spectre/Meltdown, etc).

Cloudy with a chance of misconfigurations

- Cloud security challenges aren't new, but may require some new approaches
  - Inventory and patch management
  - Managing secrets
  - Network security (firewalls, transport protection)
  - Identity management and AuthN/AuthZ

Containers: easy, until they aren't

- Software deployed as containers has advantages:
  - Ease of deployment
  - Dependency management
- It also has some foot-guns:
  - Vulnerabilities in dependencies
  - Updates

If it's on the Internet, it's getting attacked

- Attackers are scanning everything every day
  - They are especially interested in cloud resources, as it is an environment they understand and can easily utilize
  - Many existing tools for scanning/attacking cloud-hosted software/infrastructure
- We can use the same techniques to identify problems and fix them