Challenges with HPC security

Trevor Khwam Tabougua (GWDG)
May 24, 2023

What makes security for HPC different?

- Scale, performance, Data, Network, users access, and resource sharing
- Importance and objectives of security in HPC: CIA triad

The key security challenges

- Scalability
- Data Management
- Application Optimization
- Hardware Complexity

Performance vs. Security Prioritization

- HPC community tends to be more focused on performance optimization
- Security is overlooked or given lower priority
- The Department of Energy (DOE) is an exception to this trend
- This approach can create vulnerabilities and weaknesses in HPC systems, making them more susceptible to cyber threats and attacks.

Security policy

A security policy describes:

- What has to be secured

  e.g: access control, data, resources, etc.

- The ways to secure them

  e.g: multi-factor authentications, firewalls, encryption, etc.

It can also be aligned with regulations and standards such as NIST Cybersecurity framework, PCI DSS, ISO-27001, etc.

Key points of a security policy

- **Risk Assessment:** should be updated regularly to ensure that new risks are
- **Access Control:** guidance on access control measures, to ensure that only
- **Incident Response:** guidance on incident management, including incident