SECURING THE HPC CLOUD: MOTIVATIONS

Suhaimi Napis, PhD
Universiti Putra Malaysia
Founder, SIFULAN Malaysian Access Federation
Chief Innovation Officer, Birunisoft PLT

CSA cloud security alliance®

HPC Cloud Security Working Group (WG)

HPC Cloud Security WG

Mission Statement

To develop a holistic security framework for cloud infrastructure architected for high performance computing (HPC) needs, with the aim of securing where the cloud environment and HPC cross paths.

Working Group Co-Chairs

Andrew Howard
Cloud Team Manager, National Computational Infrastructure Canberra Australia

Ong Guan Sin
Head Of Cybersecurity, National Supercomputing Centre Singapore

Organizations Represented in WG So Far

Supercomputing Facilities

1. European Organization for Nuclear Research (CERN)
2. King Abdullah University of Science and Technology (KAUST), Saudi Arabia
3. National Centre for High-Performance Computing (NCHC), Taiwan
4. National Computational Infrastructure (NCI), ANU, Australia
5. National Institute of Advanced Industrial Science and Technology (AIST), Japan
6. National Supercomputing Centre (NSCC), Singapore
7. Pawsey Supercomputing Centre, Australia
8. Research Organization for Information Science and Technology (RIST), Japan

Academic / Research / Gov Institutes

1. Infocomm Media Development Authority (IMDA)
2. Institute for High Performance Computing (IHPC), A*STAR, Singapore
3. Kasetsart University (KU), Thailand
4. National Technological University (NTU)
5. National University of Singapore (NUS)
6. National Electronics and Computer Technology Center (NECTEC), Thailand
7. Universiti Putra Malaysia (UPM)

Cloud Service Providers with HPC Offerings

8. Amazon Web Services (AWS)
9. Microsoft

Solution Providers

1. Checkpoint
2. Cray
3. Drootoo
4. Fujitsu
5. Mellanox
6. Netweb
7. Redhat
8. Rescale
9. Securosys

Background

- Increasing complexity of different types of workload has resulted in the diversity of infra architectures to serve them; with cloud environments now viable to process certain HPC workloads

- However, amongst all the demonstrated efficacies that cloud has brought about, researchers face certain challenges running HPC in a cloud environment

Security of Traditional HPC vs HPC Cloud

Traditional HPC

- Typically run in highly constrained environments
- Does not have external communications capabilities by default → have small attack surfaces.

HPC Cloud

- Broad network access and
- Broad accessibility are key features.

HPC Cloud security thus needs to be viewed with a different lens and treated differently compared to **Traditional HPC.**

Technical Challenges

- Due to high performance requirements of HPC workloads, ‘close to metal’ operations are often demanded, stretching the processor’s core physical compute resource to its utmost capabilities.
- Running on a virtualized hypervisor may cause performance to suffer
- Availability (or lack) of high-speed interconnect can affect HPC’s performance

Security Challenges and WG Motivations

- Increasingly, with pure HPC bare metal infra interacting with the cloud, coupled with the evolving threat landscape, there will be more opportunities for malicious attacks.
- However, high performance faces the peril of being compromised when precious resources are carved out for security protocols and processes
- The crossing of cloud and HPC environments often leads us to questions of how security in an HPC cloud environment can be implemented, enforced and ensured without the need to compromise performance
- The WG strives to provide recommendations that can answer these questions

How to Better Secure the Workloads?

1. Limit communication capabilities of HPC applications & workloads

2. Automate workloads and security provisions as much as possible

3. Monitor everything – what is running, who has access to what etc

WG Scope

The scope for the HPC Cloud Security working group includes, but is not limited to:

- Develop a set of security guidelines for cloud infrastructures architected for HPC needs
- Develop holistic security framework covering HPC cloud infrastructure and pure HPC bare metal infrastructure; and also on-premise infrastructure overflowing to public cloud infrastructures
- Develop reference models for secured HPC cloud implementation
- Share with other HPC thought leaders in the region

HPC Cloud Security Working Group

1. Most HPC centers are working in silos, so security practices are not openly shared.

2. First need to gain better understanding of the landscape and current practices

3. Then move on to work on security recommendations for HPC cloud

Current Progress

Deliverable: **State of Security Practice in the Industry**

Provide background of HPC / HPC Cloud Industry

- Current security practice
- Challenges faced by different HPC centers

Current Progress

Deliverable: **State of Security Practice in the Industry**

Via a survey:

- Determine **level** and **type** of security that is used across HPC / HPC Cloud infrastructures
  - What are the security practices / best practices used to secure their HPC / HPC Cloud infrastructure?
  - How secure are they?

Additional Areas Suggested to Consider & Address

These were suggested during introductory calls with current WG members, or received as part of the open peer review process for the WG Charter:

- Clear definition of HPC – There is currently a broad definition, seen differently through the lens of HPC purists and Cloud Security Providers
- Infrastructure security
- Network security
- Application security
- Identity management

Identity and Access Management

- A Trust Framework/Identity Vetting based on ability to login from home institution

- REFEDS (the Research and Education FEDerations group) is to be the voice that articulates the mutual needs of research and education identity federations worldwide (https://refeds.org/)

- eduGAIN interfederation service connects identity federations around the world, simplifying access to content, services and resources for the global research and education community. (https://edugain.org/)

- China https://www.carsi.edu.cn/, India http://parichay.inflibnet.ac.in/, Japan https://www.gakunin.jp/en-fed/, USA https://incommon.org/, Australia https://aaf.edu.au/, Singapore https://www.singaren.net.sg/SGAF, Malaysia https://sifulan.my/

ASEAN Federated Identity Login Management (FILM)

- A project proposed by Malaysia to ASEAN HPC Facilities Taskforce under ASEAN Committee on Science, Technology and Innovation

- Developing the trust framework model that can be used for accessing shared research infrastructure (HPC, cloud, storage and applications)

- As first layer of security to vet the identity of users (ie users with the right trusted credentials) to be allowed to proceed to the second layer of security

- Moving away from traditional certificate based access

Certificate-Based Access and Hybrid

- Certificate Authorities facilitate certificate-based access (eg: https://www.igtf.net/, https://www.eugridpma.org/, http://www.apgridpma.org/CA/CertificateAuthorities.html

- CILogon (Cyber-Infrastructure Logon)

➔Connect application(s) using OpenID Connect, SAML, X.509, and/or LDAP, and manage attributes, groups, policies, and workflows for your collaboration, https://www.cilogon.org/

Be A Part of the Solution!

- We encourage HPC players from the international arena to join the WG
- Join us by submitting your info via https://bit.ly/2Ymq7Im or contact csa-apac-research@cloudsecurityalliance.org
- Updates on events that are related to HPC Cloud will be communicated on the WG's Basecamp and via https://www.csaapac.org
- We look forward to seeing you on the WG and at future events!

TRUST

SIFULAN

MALAYSIAN ACCESS FEDERATION

https://sifulan.my

Powered by:

Birunisoft

INNOVATION AFTER INNOVATION

suhaimi@birunisoft.com