anila.ghazanfar@gwdg.de

Anila Ghazanfar

Security and security policies

Table of contents

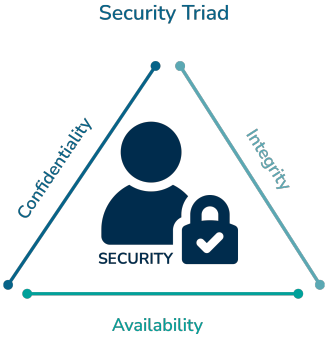
Learning objectives

- Understand the security risks associated with HPC systems
- Understand the importance of a security policy, and its alignment with ISO-27001
- Get familiar with security best practices
- Determine security issues of a service, and implement some solutions

What makes security for HPC different?

- Scale, performance, Data, Network, users access, and resource sharing
- Importance and objectives of security in HPC
  - Confidentiality
  - Integrity
  - Availability

This distinctive characteristics brings both opportunities and **challenges**.



Hou et al., "Autonomous Security Mechanisms for High-Performance Computing Systems: Review and Analysis"

Challenges

- Scalability
- Data Management
- Application Optimization
- Hardware Complexity

These challenges can also be the source of security threats.

Common HPC security threats

- Cyberattacks: malware, ransomware, phishing, Software bugs or Zero-day vulnerabilities
- Insider threats (e.g. employee misconduct): intentional or accidental data leaks, malicious software installation, or unauthorized access to sensitive data

That can lead to:

- Distributed denial of service (DDoS) attacks
- Data breaches
- Cryptocoin mining

These threats can be addressed by implementing a good **security policy**.

Bendovschi, “Cyber-attacks–trends, patterns and security countermeasures”

Security policy (1/3)

A security policy describes:

- what has to be secured
  e.g: access control, data, resources, etc.
- the ways to secure them
  e.g: multifactor authentications, firewalls, encryption, etc.

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

Security policy (2/3)

"***ISO-27001*** *(or ISO/IEC 27001:2013) is an international standard to manage information security. The standard was originally published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in 2005.*"

The GWDG is certified against ISO 27001.

ISO/IEC 27001

Security policy (3/3)

Here are three key points of a security policy that aligns with the ISO 27001 standard:

- **Risk Assessment:** should be updated regularly to ensure that new risks are identified and addressed
- **Access Control:** guidance on access control measures, to ensure that only authorized users are granted access to the system
- **Incident Response:** guidance on incident management, including incident reporting, analysis, and response

Security best practices (1/2)

Some best practices can be obtained from the security policy:

- **Password management:**
  - Aim for a passphrase
  - Do not reuse it across multiple accounts
  - Use a password manager e.g Pass, KeepassXC, Gopass, etc.
- **2-Factor Authentication:**
  - Phone
  - YubiKey
- **Secure Connections:**
  - SSH
  - SSH tunnel
  - Reverse proxy

Security best practices (2/2)

- **Data Protection:**
  - Do not copy or store data outside the HPC system unless it is necessary and is done securely
  - When working with sensitive data, encrypt data in transit and at rest
- **Software installations and Updates:**
  - Use internal or external trusted repositories
  - Updates are restricted to authorized admins
- **Awareness and Compliance**
  - report suspicious activities
  - report phishing emails: AKTUELLE PHISHING-E-MAILS
  - Participate in security training and awareness programs
  - Follow all established security policies and procedures

Example with GitLab

GitLab is web-based Git repository manager that allows teams to collaborate on code, track issues, and manage software development projects. Some security implications and solutions:

- **Authentication and Authorization:** 2-FA
- **Access control:** roles (owner, maintainer, developer, or guest), access tokens (to authenticate external applications or services), visibility (private, internal, and public)
- **Secure Communication:** HTTPS, and SSH communication
- **Secure code review:** branching, review request, review tools
- **Vulnerability management:** SAST, DAST, Security Dashboard, etc.

Exercises

Download the exercise sheet from the course web page, and follow the instructions.

References

Bendovschi, Andreea. “Cyber-attacks–trends, patterns and security countermeasures”. In: *Procedia Economics and Finance* 28 (2015), pp. 24–31.

Hou, Tao et al. “Autonomous Security Mechanisms for High-Performance Computing Systems: Review and Analysis”. In: *Adaptive Autonomous Secure Cyber Systems*. Ed. by Sushil Jajodia et al. Cham: Springer International Publishing, 2020, pp. 109–129. ISBN: 978-3-030-33432-1. DOI: 10.1007/978-3-030-33432-1_6. URL: https://doi.org/10.1007/978-3-030-33432-1_6.

ISO/IEC 27001. https://en.wikipedia.org/wiki/ISO/IEC_27001.