# Best practices for Security Management in Supercomputing

**Urpo Kaila**, *CSC – Scientific Computing Ltd.*

**ABSTRACT:** *In all areas of IT we can see increasing threats endangering the three classical objectives of information security: confidentiality, integrity, and the availability of systems, data and services. At the same time, governments are increasing the pressure to comply with proactive security measures and security related legislation. Trouble also arises from the increasing complexity of technology, customer organisations and services provided, and a demand for better efficiency, and ease of use. How does all this apply to Data Centers providing supercomputing services? How does and how should supercomputing security differ from security for "normal" computing? All the basic security principles do apply to supercomputing as well. Risk analysis should be made, requirements should be understood, physical, technical, and administrative security controls should be implemented and audited. We present a top-down overview on how to implement good practices of information security management in supercomputing and suggest more international security-related collaboration in comparing and benchmarking information security practices for supercomputing.*

**KEYWORDS:** security, best practices, supercomputing, data center

## 1. Introduction

Threats for IT services in general have increased over time. Intelligent tools for automating attacks against systems and services has developed and become freely available. A good example of the powerfulness of the current attacking tools is toolsets available through the Metasploit project, which develop tools for penetration testing. Without much technical skills, it is possible to perform advanced, adapted and automated attacks against a large number of targeted hosts. As we can daily see from our system logs, many kinds of malevolent scanning and probing proves how widespread and global the use of attacking tools is. Trails of unsuccessful login attempts can be found from both our local constituent networks and from traditional areas for crackers as some networks in China, Romania, Brazil and Russia, just to mention a few.

We should naturally be more worried about those attacks which don't leave trails. In such case somebody might have been able to break in to the system, steal a user account and install a backdoor, or worse, a rootkit. A rootkit hides itself from system administration but gives intruders root access to the infected system.

Increasing complexity of IT systems makes them also more vulnerable against attacks but also against errors and faults. The complexity has increased both in a technical sense, with more interdependent services but also in a organisational sense. Technical complexity has increased alongside of adding new features to operating system kernels and applications, middleware and user application software. By following up the number of known vulnerabilities, it is easy to see that the experts and teams securing systems, has more threats to take care of.

| Year | Total vulnerabilities catalogued |
|---|---|
| Q1, 2008 | 1,474 |
| 2007 | 7,236 |
| 2006 | 8,064 |
| 2005 | 5,990 |
| 2004 | 3780 |
| 2003 | 3784 |
| 2002 | 4129 |
| 2001 | 2437 |
| 2000 | 1090 |
| 1999 | 417 |
| 1998 | 262 |

Table 1. Total vulnerabilities catalogued. © CERT/CC. 2008.

The complexity of system administration has increased also because of organisational and business reasons. The number and variety of systems to manage, outsourcing partners, subcontractors and peer networks of interdependent systems increases and the constant business pressure for efficiency and change creates challenges of it own.

## 2. What was information security all about?

According to the current and well know definition, information security means protecting systems, data and services on

- Confidentiality
  - To prevent intentional or unintentional disclosure
- Integrity
  - To prevent unauthorized modification and protects consistency
- Availability
  - To protects reliable and timely access

People might associate information security only with confidentiality or with computer security. According to taxonomy in the ISO/IEC 27002 standard, the code of practice for information security management, information security should cover the all following areas:

- Risk assessment and treatment
- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

As we can see, the field covers a wide are technical and administrative topics

Information security measures must always be based on identified risks and assets to be protected.

Information Security is a management responsibility, not only a task for the technical experts. Without management commitment there will not be resources available for proper controls and operations. On the other hand, without skills and understanding in IT systems and system administration, security measures might dilute to just bureaucracy.

Information security is practiced through controls, which can be physical, technical or administrative security controls. The controls should be developed by an iterative Plan-Do-Check-Act cycle.

Finally, information security should be a part of quality assurance, not only a compliance requirement.

## 2. Security and business needs

A typical business vs. security issue is when you for example have to decide when to patch known kernel vulnerability. Your users hate the boot but the risk of system compromise with risk for root kits and backdoors might be still worse.

If the requirement for confidentiality sometimes might be perceived as far fetched by the management, the requirement for availability of systems and services can be intuitively understood by almost everybody.

Availability, which can be measured in “number of nines” of planned and/or none planned outages. One should not let oneself to be misleading by the metrics. For users of supercomputers, who submit jobs lasting for weeks, one second outage can mean a loss of one month’s job!

| Availability | Downtime p.a. |
|---|---|
| **95%** | **18.25 days** |
| **98%** | **7.30 days** |
| **99%** | **3.65 days** |
| **99.5%** | **1.83 days** |
| **99.8%** | **17.52 hours** |
| **99.9%** | **8.76 hours** |
| **99.99%** | **52.6 min** |
| **99.999%** | **5.26 min** |

Table 2. The classical availability table.

Security must support business! Although security in general and information security in particular is often misunderstood to be a hindrance for business and limiting operations security controls are for supporting and enabling business.

‘Low security’ can mean just bad quality, but of course, also ‘high security’ can also my mean awkward usability and outdated services. Too much or too little security is bad security.

The requirements for compliance with laws, regulations, contracts and best practices are generally getting tougher. Management and systems administrators are more and more frequently being audited for compliance. Surviving security audits by has for many organizations become a major business issue. At the end of the day, security is about managing trust.

The ends of business and security requirements meet in a most natural way in risk management. During risk assessments management and technical experts should jointly identify assets and services to be protected and related threats and vulnerabilities. The risk assessment should result in a forecast of risks and

| | |
|---|---|
| Threat: | Intruder breaks in Cray XT4 louhi.csc.fi |
| Vulnerability: | Unpatched ssh-demon on Louhi frontend |
| Risk: | Likelihood of malevolent intruders cracking Louhi. |
| Exposure/ Impact: | Service outage for two weeks while reinstalling louhi due rootkits, A loss in trust for system and service administration |
| Safeguard: | Patch ssh-demon, implement and monitor patch management |

Table 3. Example of risk assessment.

The demand for a development of speed and throughput and ‘more bits for the bucks’, economic and technical efficiency makes both system development and security administration an interesting challenge.

The need for greater flexibility, a faster pace of change and easy ubiquitous system access can be difficult challenges for information security management.

Many of the classical security controls, as listed, for example, in the NIST listing of generally accepted good security principles, are difficult to implement without endangering flexibility and easy access for users and administrators alike. Such security principles are:

- External systems are insecure
- Implement layered security
- Isolate public access systems from mission critical resources
- Implement boundary mechanisms to separate computing systems and network infra

Especially implementing physical security controls seems to contradict the requirements for flexibility and easy access.

Despite all challenges in implementing security controls, at least the senior management are always liable for compliance and proper corporate and IT governance.

## 3. Does supercomputing differ?

Does requirements and implementations of information security for supercomputing differ from other kind of IT services?

The following list is a simple comparison of differences and similarities:

Differences with other IT services

- Experimental, cutting (bleeding?) edge technology
- A small amount of users
- Users do not pay for the service themselves
- Jobs not time critical, can be repeated in case of outages
- Very high costs per users
- Often public funding

Similarities with other IT services

- All the same threats and some more
- Requirements for efficiency and quality rising
- Delivered as a service, not as art
- Dependent of infrastructure and subcontractors

According to our own, limited experiences from the CSC site, especially following security measures might need some special care and improvements:

- User management and user access rights management
- Controlling root access
- Remote administration

- Controlling system integrity, or at least the ability to do it
- Incident handling and disaster recovery
- Network security
- Patch and configuration management
- Security should be a normal part of the job, not a hobby to do if and when you have time and interest

## 5. Conclusions

In our presentation, we have tried to show, how increasing threats and requirements for generic compliance might be difficult but necessary to manage. The site administration needs to please the security auditors and users alike and balance between adequate security measures and user experience of easy and flexible access.

Information security for supercomputing sites should and can be improved with reasonable resources. Better security controls could be developed more efficiently and with better results, if it could be done together in cooperation with vendor and with leading peer sites.

Security controls are investments which must pay off

Also supercomputing needs to comply with laws, regulations and contracts. All the basic security principles do apply to supercomputing as well. Risk analysis should be made, security requirements should be understood and physical, technical, and administrative security controls should be implemented and audited.

It is the responsibility of the management to see that the experts can and will take care of security.

With limited resources and tight schedules it is often difficult to identify and prioritise security measures. The fact is, that less severs risks must just be consciously taken, and the site should bear the risk residual.

Also, we do need better security tools, customised for supercomputing. A preliminary wish list could be

- Automated vulnerability and patch management
- Proactive and automated log monitoring
- Trustworthy implementations of IDS/IPS and system integrity checks
- More waterproof controls for access rights and user management
- Better communication for administrators, site security and CERT/CSIRT teams
- Skip finally login with passwords, use keys or certificates
- Partitioning the user (data) space
- Tools for detecting and reporting scans and queries

## 6. Suggestions for how to improve security together

We suggest, based on our conclusions above that:

- A joint project sharing and developing best practices for information security in supercomputing should be started

- Security benchmarking should be initiated among leading for Cray sites: availability, incidents, scan results and implementation of controls

- In the future, peer auditing could help to improve security

## Acknowledgments

The authors would like to thank colleagues at CSC for trying to improve security together and helping to formulate the ideas presented in this paper.

## About the Author

Urpo Kaila is IT Security Manager at CSC – Scientific Computing Ltd. He is managing and developing information security measures for IT services in CSC and Funet, the National Research and Education Network (NREN) in Finland. He is involved in projects related to information security for supercomputing and grid computing, risk analysis, business continuity and implementing strong authentication at universities.

He is also a member of the Computer Security Incident Response team Funet CERT and board member of Finnish Information Security Association. He has just started to prepare PhD thesis at on Helsinki University of Technology on ‘Beyond Best Practices for Information Security Management in NRENs’.

Urpo can be reached at CSC – Scientific Computing Ltd., P.O. Box 405 , FIN-02101 Espoo, Finland. Email: urpo.kaila@csc.fi