Best practices for Security Management in Supercomputing

Cray User Group meeting, CUG 2008
Helsinki, Finland
2008-05-05

Urpo Kaila <urpo.kaila@csc.fi>
CSC - Scientific Computing Ltd.

Agenda

- **Introduction**
  - The CSC site
- **What was Information Security all about?**
  - The CIA Model
  - Security Controls
  - Best practices for information security
  - Compliance and Risk Management
- **Business needs**
  - The ubiquitous customer
- **How does supercomputing differ?**
  - Some cases, some incidents
- **Suggestions for how to improve security together**
  - Benchmarking Security
  - Sharing and developing best practices

The CSC site

CSC

- Is the Finnish IT center for science
- Is a non-profit company
- supports the national research structure
- has a staff of about 160 persons
- as part of the Finnish national research infrastructure, develops and offers high-quality information technology services
- provide services for universities, research institutions, polytechnics, companies & government

CSC's services

- Funet services
- Computing services
- Application services
- Data services for science and culture
- Information management services

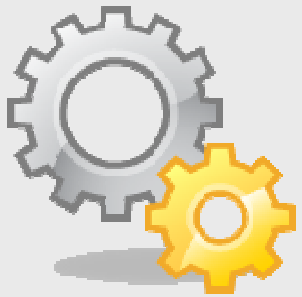
- **louhi.csc.fi -> Cray XT4**

also other hosts for computing services

- **murska.csc.fi -> HP CP4000 BL ProLiant super cluster**
- **sepeli.csc.fi -> HP ProLiant DL145 Cluster**
- **corona.csc.fi -> Sun Fire 25K application server**

CSC

CSC Facilities



- **Life Science Centre 3**
  - High availability, high performance secure hosting facilities
  - 460 kW redundant cooling capacaity, Floor space 1000 m2 including technical infrastructure
  - 85 % of cooling capacity in use (April 15, 2008)
- **Life Science Centre 5**
  - High availability high performance secure hosting facilities
  - 800 kW redundant cooling capacity
  - In production during the summer 2008
- **Hosting and security services**
  - Proactive and planned maintenance is the prerequisite for high availability
    - Electricity, cooling, automation
    - Fire protection systems
    - Access control systems, CCTV
    - Planning and change management
    - Outsourcing and subcontracting
    - 24/7/265 HVAC monitoring

CSC and security

CSC and FUNET are part of national critical infrastructure

- FUNET is the Finnish NREN
- Core computing services
- The library services
- TLD services for FICORA

Organising internal security

- **Information Security Policy and guidelines**
- **Security organisation**
  - The role of senior management
  - The role of experts and middle management
  - The security group
- **Incident response**
- **Physical security and safety**
- **Protecting privacy**

FIRST Forum of Incident Response and Security Teams

Networking and providing security services

- Funet CERT – the first CERT team in Finland
- The Security groups for FUNET constituents
- TF-CSIRT and FIRST
- Grid Security, see for example: https://extras.csc.fi/mgrid/sec/

registered by TRUSTED Introducer The European CSIRT Directory

CSC

What was information security all about?

Information security is about 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

<u>based on risks and identified assets to be protected</u>

CIA

Do not forget!

Physical, Technical and Administrative Security Controls

- Deterrent
- Preventive
- Corrective
- Detective

Information Security is

- ❑ a fundamental part of total quality
- ❑ management responsibility
- ❑ implemented by iterative controls

☞ Corporate security should "own" policies, auditing and incidents, <u>the teams</u> are responsible for controls and monitoring

Availability ABC

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

```
louhi-login8 csc/user> xtshowcabs

Compute Processor Allocation Status as of Tue Apr

     C0-0     C1-0     C2-0     C3-0     C4-0
  n3 jjeeeeea aallllo iaammmmm fffkmmmm mmmmjjjj
  n2 jjeeeeea aallllo iaammmmm fffkmmmm mmmmmjjj
  n1 jjjeeeea aallllo iiaammmm ffffmmmm mmmmmjjj
c2n0 jjjeeeea aallllo iiaammmm ffffkmmm mmmmmjjj
  n3 ;;jjjjjj aaaaaaaa liiiiiii qqnnffff mmmmmmmm
  n2 ;;jjjjjj aaaaaaaa liiiiiii qqnnffff kmmmmmmm
  n1 ;;ljjjjj aaaaaaaa lliiiiii qqnnffff kmmmmmmm
c1n0 ;;fjjjjj aaaaaaaa lliiiiii qqnnffff kmmmmmmm
  n3 SSSSSS;; SSSSSaaa oooooool mfqqqqqq mmmmmmmk
  n2       ;;      aaa oooooool mmqqqqqq mmmmmmmk
  n1       ;;      aaa oooooool mmqqqqqq mmmmmmmk
c0n0 SSSSSS;; SSSYSaaa oooooool mmqqqqqq mmmmmmmk
    s01234567 01234567 01234567 01234567 01234567
```

- In the real world, it do take time to rerun your jobs after an (planned or not) planned outage! One second outage, one months job, for example!
- Premiere Gmail (50 $/ year/account) guarantees 99,9% uptime
- What would be the proper availability for computing services?

Compliance and Best Practices

Minimum level of security

- Comply with national laws, government regulation and contracts
- Privacy and security laws
- In Finland, the requirements for compliance are getting tougher
  - More auditing
  - Security becomes a part of contracts

☞ **Optimal level of security**

- Security supporting business
- The warm an fuzzy feeling of reasonable trust and quality

☞ **Non-Optimal level of security**

- Too much or too little security is bad security
- "low security" can also mean just bad quality
- "high security" can mean awkward to use

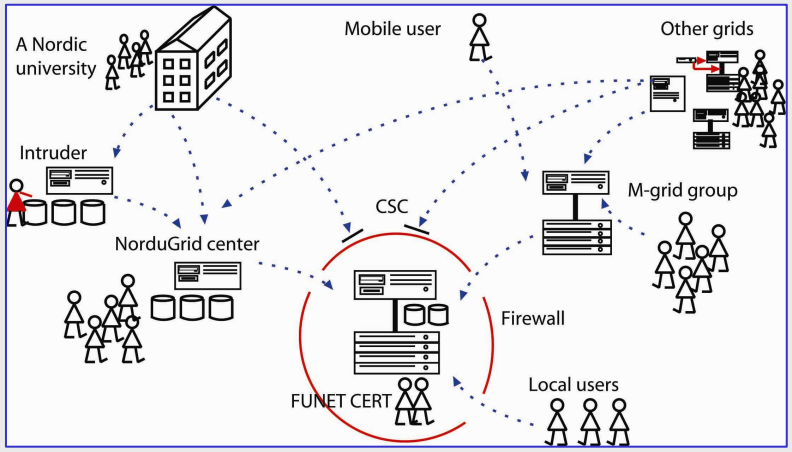
Several interrelated best practices for IS and IM

- COBIT
- ISO27001 and other IS027*
- ISM3
- ITIL
- (ISC)2 CBK

CSC

NIST (selected*) Security Principles (800-27)

- Establish a security policy
- Security as an integral part of the overall system design
- External systems are insecure
- Identify trade-offs between risk and costs
- Implement layered security
- Avoid single points of vulnerability
- Minimize the system elements to be trusted
- Isolate public access systems from mission critical resources
- Implement boundary mechanisms to separate computing systems and network infra
- Authenticate
- Ensure access control
- Use unique identities
- Implement least privilege



Picture for Mgrid Secwg by Arto Teräs/ CSC

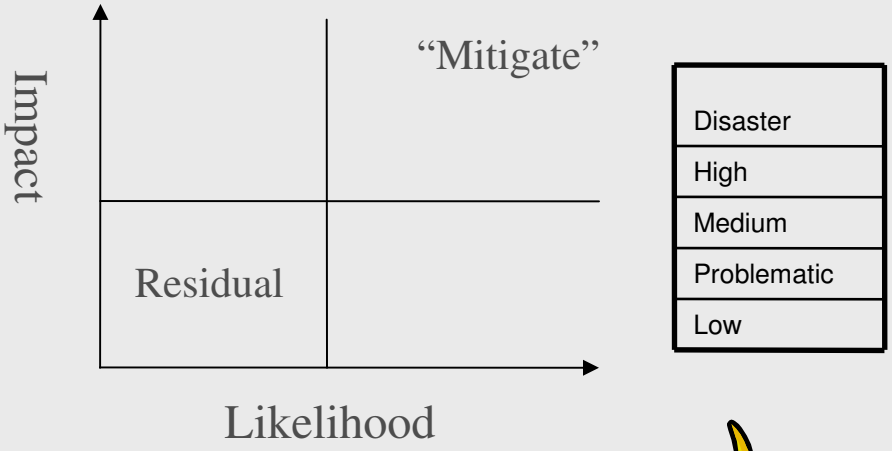
Attention! Danger of lagging behind

Need continuous effort!

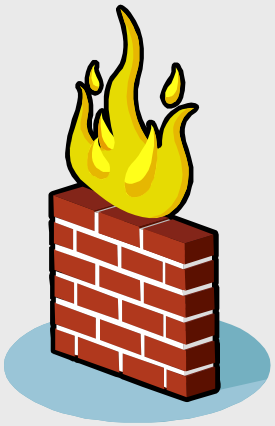
* 33 good principles => http://csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf

Risk Management

Risk = likelihood x impact (the classical formula)



- Fire
- Sharing account
- Lack of monitoring
- Misuse of resources
- Infrastructure problem
- Regulatory requirements
- Lack of required skills
- Change management problems



TERMS

Threat:

Hacker breaks in on Louhi

Vulnerability:

Unpatched ssh-demon on Louhi frontend

Risk:

Likelihood of a hacker cracking Louhi

Exposure/ Impact:

Service outage for two weeks while reinstalling louhi due rootkits, PR loss

Safeguard:

Patch ssh-demon, implement patch management

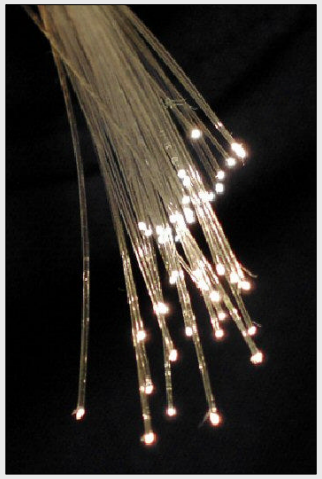
Business needs

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

Security must support business

Ubiquitous supercomputing needs to be

- Fast and flexible
- Easy to use
- Affordable
- Powerful
- Reliable and secure
- Best of breed
- services instantly accessible from everywhere



Sourcing and networking increases complexity & dependence

Technical challenges

- The demand for speed and throughput
- Interdependences of systems
- Managing trust

IT Governance

- More bits for the bucks
- Compliance
- Risk avoidance

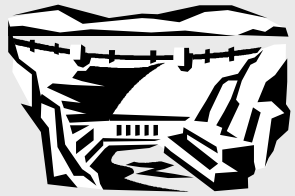
How does supercomputing differ?

- **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

CSC

What have we learnt so far? (from the information security point of view)

Leanings from some incidents by us and by some other sites after:

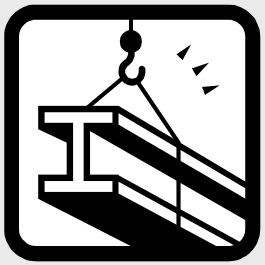


- **System compromises**
- **Vulnerabilities**
- **Privacy issues**
- **Flood and fire**
- **Electricity and cooling issues**
- **Malfunctions**
- **Compliance issues**
- **Integrity problems**
- **Spam and phising**
- **Denial of Service**
- **Insecure configuration**
- **Scans and queries**

- Proper planning and system administration do pay off
- We cannot patch all vulnerabilities, check all logs or hunt all scanners
- Cooperation between technical experts and service management is a must
- Auditing shows that we do all read the same ISM textbooks
- Cray takes better care of patching vulnerabilities than some other vendors
- Good information and cooperation helps a lot
- No resources without management commitment

CSC

How to improve security together (1/2)



- **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:**
  - User management and access rights
  - 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**
  - **It is job of the management to see that the experts can and will take care of security**

Could the best practices be better (1/2)?

- **Everybody has too much to do…**
  - It is often difficult to identify and prioritise
  - Less sever risks must be taken, that is the risk residual
    - For example ssh scans for bad user passwords

- **We need better security tools!**
  - Trustworthy implementations of IDS/IPS and system integrity checks
  - Proactive and automated log monitoring
  - Waterproof controls for access rights and user management
  - Automated vulnerability and patch 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
  - Detecting and reporting scans and queries

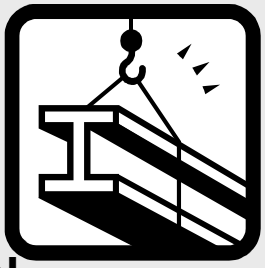
Could the best practices be better (2/2)?

- **The checklists for the ISM Best practices are really exhaustive**
  - 350+ controls in ISO 27001?!?
  - 20/80 rules do apply

- Security through social networking
  - The bureaucratic tone of information security must be turned to ….
  - …the Agile Administrator and resilience
  - Security is primarily the task of the administrator and service manager
  - A new, more supportive and communicative role for site IT Security

How to improve security together (2/2)

- **Information security for supercomputing sites should and can be improved with reasonable resources**
- **Security controls are investments which must pay off**
- **Also supercomputing need to comply with laws, regulations and contracts**
- **The management top-down view must meet the technical bottom up view**



<u>Suggestions:</u>

- **A joint project 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**

CSC

Thank you!

Comments, feedback, questions?