Security Update and Risk Assessment

Mingchao Ma

STFC - RAL, UK

HEPSYSMAN Workshop

22nd November 2010

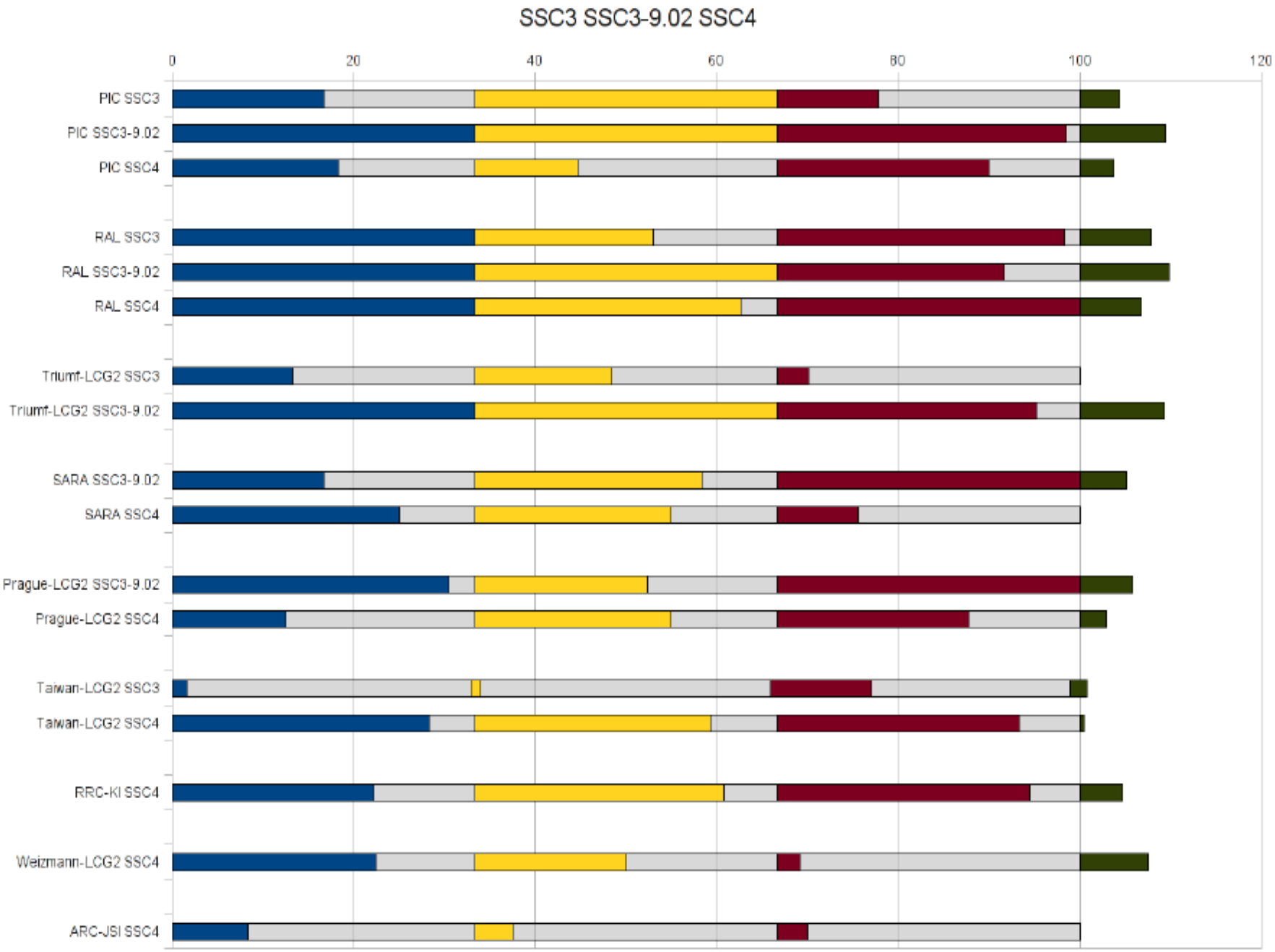
Overview

- Security Update
- Risk Assessment
- Discussion

Security Update

- Operational Security Procedures
  - Security incident handling procedure and Vulnerability issue handling Procedure
    - https://documents.egi.eu/document/47
  - EGI CSIRT Information Disclosure Policy (draft)
    - https://wiki.egi.eu/wiki/EGI_CSIRT_Information_Disclosure_Policy_(draft)
  - Working on Critical Vulnerability Handling Procedure

Science & Technology Facilities Council


SSC3 SSC3-9.02 SSC4
0
20
40
60
80
100
120
PIC SSC3
PIC SSC3-9.02
PIC SSC4
RAL SSC3
RAL SSC3-9.02
RAL SSC4
Triumf-LCG2 SSC3
Triumf-LCG2 SSC3-9.02
SARA SSC3-9.02
SARA SSC4
Prague-LCG2 SSC3-9.02
Prague-LCG2 SSC4
Taiwan-LCG2 SSC3
Taiwan-LCG2 SSC4
RRC-KI SSC4
Weizmann-LCG2 SSC4
ARC-JSI SSC4

Security Update (3)

- Security Monitoring
  - EGI Pakiti: https://pakiti.egi.eu
  - Site/NGI security officers can now access Pakiti result
- Security Dashboard Development
  - EGI CSIRT will be able to access all security monitoring results at one place
  - Will integrate with EGI CSIRT ticket system
  - Will integrate with EGI/NGI operation dashboard
    - Working with operation dashboard developers
  - Will allow CoD/RoD to view the security alerts and follow up with sites
    - Need to discuss it with CoD/RoD team in due course

Security Update (4)

- Since 1st May 2010 (start of the Project)
  - EGI CSIRT has handled 5 security incidents
  - EGI CSIRT has issued 9 security advisories, of which
    - 2 Critical
    - 4 High
    - 3 Moderate

    https://wiki.egi.eu/wiki/EGI_CSIRT:Alerts
  - Risk assessment now follows SVG procedure and joint assessment of CSIRT and SVG

Science & Technology Facilities Council

Risk Assessment

Assessing risk and taking steps to reduce risk to an **acceptable level**

Science & Technology Facilities Council

Risk?

- Risk is a function of the **likelihood** of a given **threat-source's** exercising a particular potential **vulnerability**, and the resulting **impact** of that adverse event on the organization.*

* NIST SP800-30: Risk Management Guide for Information Technology Systems
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Science & Technology Facilities Council

Step1: Know Yourself

- Know your system
  - Hardware
  - Software
    - OS, Middleware, Patch level etc.
  - Network Topology
  - Any critical system
  - Any users (local & external)
  - … …
- Monitoring tools
  - Pakiti, Nagios etc.

Step 2: Know Your Enemy

- Threat that we are facing
  - Internal users or external attacker?
  - Opportunistic attack?
  - Targeted attack?
    - Targeted the Grid?
  - Sophisticated and targeted attack?
    - Customized malware tailed for the targeted environment only?
    - Targeted the Grid?
- History of security incident
  - Both local and the Grid incidents

Step 3: Vulnerability

- Understand the Vulnerability
  - Is the vulnerability exploitable?
  - Is it locally or remotely exploitable?
  - Can it be exploited by authorized users only or not?
  - How can it be exploited or under what condition it can be exploited.
  - What level of knowledge/skills are required to exploit it?
  - Is there reliable public exploit out there?
- Security Advisories from EGI CSIRT

Step 4: Control Analysis

- Any existing/deployed control mechanism in place that might mitigate the risk
  - Firewall
  - IDS/IPS

Step 5: Likelihood determination

- Based on the information gather from step 1-4
  - High
  - Medium
  - Low

Science & Technology Facilities Council

Step 6: Impact/Consequence

- The consequence if system being compromised
  - One host unavailable?
  - Some service interruption?
  - The whole site down?
  - Affect other sites?
  - Incident propagation?
  - Cost (operational cost) to correct the problem?

Science & Technology Facilities Council

Step 7: Risk Determination

- Based on Likelihood, Impact and any controls in place
  - Critical
  - High
  - Medium
  - Low

Science & Technology Facilities Council

Step 8: Risk Mitigation

- Reduce risk to an acceptable level
- Need to take into account of operational cost when mitigate a risk

Discussion

- Security vs. availability
- Operational cost when mitigating a risk (e.g. kernel update)
- No procedure in place to assure the quality of risk mitigation
  - No check after risk mitigation
  - No clear responsibility