Policy & Security Issues For Class 2/3 Virtual Machines

Ronald Starink

BiG Grid Virtualization Working Group

Introduction

- Investigation policy & security issues for
  - Class 2 virtual machines ('VO-provided')
  - Class 3 virtual machines ('user-provided')
- Focus:
  - Why problem for BiG Grid but not e.g. Amazon?
  - Difference VM and regular grid jobs?
- Results from discussions with sysadmins and security staff

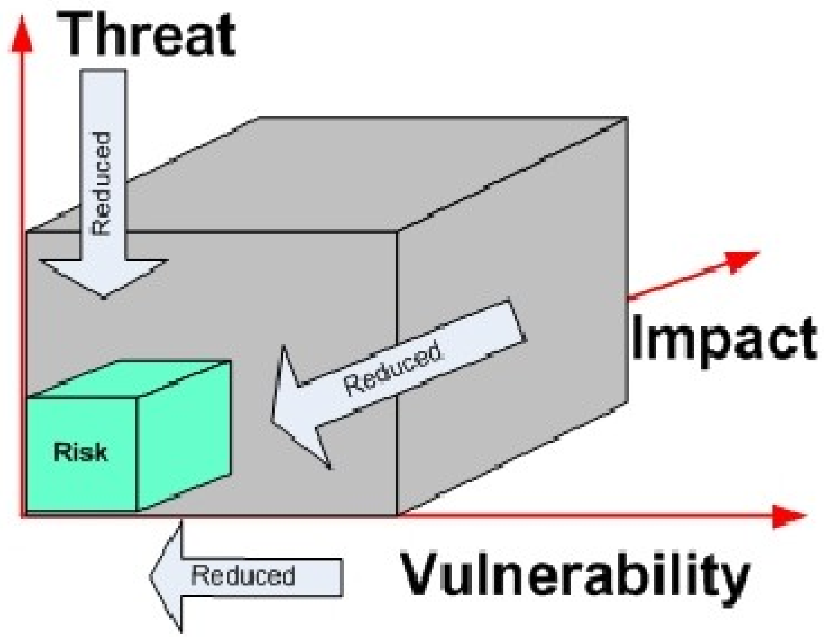
Responsibilities of Operations

- Operation of generic grid infrastructure
  - BiG Grid: added value, not just bunch of CPU and disk
- Assure:
  - Service availability for all legitimate users
  - Data integrity, confidentiality / privacy
  - Non-repudiation of user actions

    (relate user action to individual)
- In case of incident: forensics required
  - Legal actions
  - Fix vulnerability before system operational again

Security: Risk

- Risk = Threat x Vulnerability x Impact
  - Threat = attackers
  - Vulnerability = platform
    - OS, services, applications
  - Impact = exposure, gain



- Reduce to *acceptable* level
  - Technical measures
  - Policies

(source: Peter Jackson, 'Grid Security')

Risk and Class 2/3 VMs

- Many potential vulnerabilities
    - Unknown OS patch level
    - No distinction user vs privileged accounts
        - UNIX uses latter to mitigate risks
    - VM software layer adds risk (all VM classes)
        - Compromised VM: root access to host and then to other VMs
- Risk reduction
    - No network connectivity (*threat*)
        - Still vulnerable to malicious users / unprotected VM repositories
    - Certification by trusted experts (*vulnerabilities*)
        - Only accept certified VM
        - Considerable effort

Manageability Class 2/3 VMs

- Site admins cannot easily access VM to check
  - *Nor trust what they see if they get in!!!*
- Incident → forensics on VM
  - Impossible
    - VM image not saved or possibly corrupted by attacker
    - Black box approach: too expensive
- Incident response much more expensive than certification

Comparing BiG Grid and AWS

- Amazon Web Services:
  - Prepared environment not relying on privileged accounts in VM
  - Lots of staff on 24x7 basis
- Incident:
  - AWS well known, no reputation damage
  - BiG Grid and its sites (mainly SARA and Philips) face serious reputation damage
  - 'Malicious' BiG Grid site → TLD may kill domain

Existing Policy: VO box

- Currently no specific VM policies
  - But VO box policy very similar
- VO box: runs VO software in user space
  - Class 1: no privileges in trusted network
  - Class 2: requires privileges in trusted network
    - Temporary solution, will be phased out
    - **NO** root access for VOs

Conclusions

- Risk for class 2/3 VMs
  - Extra risk compared to regular jobs
  - Reduction via certification? Manpower!
    - May be possible for class 2 VM
    - Not feasible for class 3 VM
- BiG Grid cannot handle publicity of incident
- BiG Grid OST: no support for class 3 VMs
  - *“The users don't really want this”*