Cloud Security Risks and their Mitigation

Linda Cornwall, STFC

WISE @ DI4R Krakow, 27th Sept 2016

www.egi.eu

Introduction

- This is in the context of the EGI federated cloud, activities within, and discussions we have had
- Some of this information is a bit sensitive, the version of the slides on the web is slightly different

EGI Federated Cloud

- The EGI Federated Cloud has been operational since May 2014
- Currently 21 Cloud Resource Centres across Europe

https://wiki.egi.eu/wiki/Federated_Cloud_infrastructure_status

  - ~7000 cores
  - cf ~650,000 cores in the 'Grid'
- Access via the OGF OCCI standard interface

http://occi-wg.org/

- The various EGI security groups are working with the EGI Federated cloud to integrate the security activities

EGI Security Threat Risk Assessment

- This activity was carried out towards the end of 2015, beginning of 2016
  - Report completed February 2016.
- Focus on the EGI Federated Cloud and the mitigations in place at that time
  - But general threats/risks included too
- Similar to the activity carried out in 2012
  - Talked about in Barcelona
  - Recently we used a similar methodology
- Work carried out in a spreadsheet, via audio conferencing, and by e-mail

Methodology

- Step 1 – Establish team
  - Not as easy as it sounds, everyone busy
- Step 2 – Draft Threat and Threat Category Selection
  - Started from version from 2012
  - Tidied and added cloud specific categories
- Step 3 – Assign team member to each category
  - Member improves list of threats
  - Establishes the current situation, mitigations in place
- Step 4 – Agree list of threats
- Step 5 – Ask everyone to go away with a spreadsheet, and rate 'Likelihood' and 'Impact' for each threat
  - between 1 and 5

Methodology (2)

- Step 6 – Gather in all spreadsheets, compute the average risk
  - For each person Risk = Likelihood * Impact
  - Then take average of the risk
- Step 7 – Discuss some of the threats
  - Those people wanted to highlight
  - Those which have a higher standard deviation in value
- Step 8 – Suggest some further mitigations
  - We needs a lot more work on the cloud specific threats
- Step 9 – Write report

1 important mitigation in the Fed Cloud

- Only ‘endorsed’ VM images are allowed to be run
  - People cannot run any image they wish
- VM images created by an expert (hopefully) and endorsed by the Virtual Organisation (VO) managers.
- This is probably the main reason we don’t get masses of incidents
- But we get incidents
  - Bad endorsed VM
  - Bad contextualization for a generic VM

Summary of results

- Selected 103 threats in 19 categories
  - Compared to 75 in 20 categories in 2012
- Some streamlining, plus added some new categories concerning the cloud
- 10 people returned a spreadsheet, all filled in all for nearly all threats
- Report 24 out of 103 have a value of 10 or more
  - Compared to 18 having value 8 or more in 2012
  - Half in this new assessment have risk 8 or more
- Risk values much higher
  - because we have less control over S/W, tech…??

4 main areas 'High' risk

- Security Incidents in the Federated Cloud
  - Detection, handling, etc.
- Software and Technology
  - Less control than in the past of what technology is in use, some may not be secure, may not be supported etc.
- Staffing levels and training
  - Insufficient staff to carry out security activities, not enough skills
- Policy and Adherence
  - People may not be aware of policy, or may ignore it, e.g. data protection

Highest Risk Threat

- Sorry not public

More Cloud specific risks

- Sorry not public

Cloud Mitigations being worked on

- Endorsed VAs is best we have
  - I reckon we would have a lot more incidents if this wasn't in place
- Contact e-mail lists for VM endorsers and VM operators
  - Don't have either of these yet
  - Useful for informing of vulnerabilities
- Software improvements for banning/suspending users
- SSC's related to the cloud

Cloud Mitigations (2)

- Connectivity restrictions
- Monitoring
- Considering VM operator role, so only those with that role can instantiate VMs
  - At present anyone who is a member of VO which is cloud enabled can instantiate VMs
  - Most work done with VMs based on very specific VAs
  - In future – imagine less privileged users will access VMs

Other highest risk threats

- Sorry not public

SW checklist

- We produced a checklist to try to make people think about what software they are writing or selecting

https://wiki.egi.eu/wiki/SVG:Software_Security_Checklist

Conclusion

- Our Security threat risk assessment wasn't as polished as it might be, but highlights a lot of the problems with federated infrastructures especially federated clouds
- Security risks are higher in the Cloud, we have less control over what people do, what software is in use, and who has privileged access
- We are doing some things in EGI to mitigate some of the risks, but collaboration with others would be great.

Report and slides

- I will send you the report and spreadsheet if you wish, and agree to treat as 'AMBER'
- Request by E-mail me - Linda.Cornwall at stfc.ac.uk

Thank you for your attention.

Questions?

www.egi.eu

Likelihood and Impact Guidelines

- No statistics to do a proper actuarial probability and cost – so have to go with judgement, gut feeling, and some guidelines
- Guide to 'Likelihood' is
  1. Unlikely to happen
  2. May happen 2-3 times every 5 years
  3. Expected to happen once a year or so
  4. Happens every few months
  5. Happens once a month or more

Guide to 'Impact' (Based on WLCG)

1. Minimal impact on EGI's ability to deliver its services to users or on any other asset.
2. Minor impact, such as some operational or financial costs, local service disruption of less than 1 week.
3. Serious localised disruption to some services for some users, for a week or more. Significant productivity loss, significant financial or operational cost. Or significant impact on other assets, such as reputation or people.
4. Serious multi-national disruption to some services to all users, for a week or more, leading to productivity loss, significant financial or operational cost. Serious damage to reputation of EGI.
5. Very serious disruption, where EGI is unable to deliver services to users for a week or more. Damage to reputation and/or third parties which may affect funding and continuity of the project.