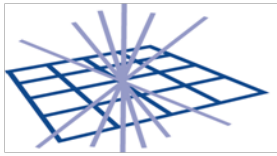
Science & Technology Facilities Council



Cloud Security

David Kelsey

(STFC-RAL, UK)

28 May 2009

HEPiX, Umea

david.kelsey at stfc.ac.uk

Aims

- Consider various security issues
  - Use of Cloud (virtual) resources in Grids
  - Also mention use of Volunteer Computing in Grids
- Trust, policy and operational issues
  - Not considering technical security issues of Virtual Machines (see Jan Iven's talk)
- Thanks to David Groep (NIKHEF) and others (OGF paper – see links)
- *Disclaimer: my personal views – not the official view of GridPP, WLCG or EGEE*

A better title?

- Cloud Security
  - Securing the “cloud”
- *Security in the Cloud*
  - Securing the services running in the cloud

Trust and Policy

- *Trust(worthy):*
  - Predictable, dependable, responsible, honest, reliable… behaviour
- Management of IT security
  - All about management of risks and balancing with availability of services
- Security Plan can include various “Controls”
  - Technical, Operational and Management
- One method of establishing Trust
  - In a collaboration of multiple admin domains
  - Written security policies

Scalable Grid Trust

- Impossible for users to register at all sites, or even for a VO to establish trust at all sites
- Grids have developed and agreed **common** security policies and best practices
  - Participants assumed (required) to be trustworthy
    - Must accept policies
    - With sanctions if they misbehave
- User registers once with VO; Site and VO registers once with the Grid

Some example Grid policy statements

- **User AUP**: You shall only use the GRID to perform work, or transmit or store data consistent with the stated goals and policies of the VO of which you are a member and in compliance with these conditions of use.

Examples (2)

- **Site Operations Policy**: When notified by the Grid of software patches and updates required for security and stability, you shall, as soon as reasonably possible in the circumstances, apply these to your systems.
- You shall comply with the Grid incident response procedures regarding the notification of security incidents.

Examples (3)

- **VO Operations Policy**: You are responsible for ensuring that your software does not pose security threats, that access to your databases is secure and is sufficiently monitored, that your stored data are compliant with legal requirements, and that your VO services, including pilot job frameworks, are operated according to the applicable policy documents.

Grids and volunteer computing

- Enabling Desktop Grids for eScience (EDGeS) project
  - E.g. Connecting BOINC volunteer nodes to EGEE
  - http://www.edges-grid.eu/
- The volunteer “worker node” (WN) is not trusted
  - Owner is not trusted either
- Delegate Grid identity (proxy certificate) from Grid to WN
    - Needed for file access (from Grid SE)
  - No technology to “restrict” the capability of the credential
  - Could be stolen and used by owner of the WN
- Cannot rely on policy agreements to control behaviour
- No acceptable solution yet

Cloud resources on the Grid

- Consider a Cloud operated by a third party – submit machine images (e.g. Amazon EC2)
  - Independent third party, not part of Grid collaboration
- There are many possible security issues
  - Not just technical – policy, trust and operational
  - These need to be addressed before connecting this Cloud to your Grid

(Some) Security Issues

- Access to the Cloud
  - When submitting the machine images
    - Trust and mutual authentication important
  - Are you talking to the correct cloud?
    - Phishing attacks
  - Re-usable authentication tokens (e.g. cookies)
    - Cross-site request forgery attacks

Issues (2)

- Data security and privacy
  - Need to encrypt data
    - But will always be a time when this is unencrypted in memory
  - Must trust the provider
    - via policy/contract or reputation
    - Data protection for handling of personal data
      - E.g. logging and accounting data

Issues (3)

- Networks and Firewalls
  - Need to open holes in your Grid firewalls
    - To allow cloud to access your site
  - Can you assume static IP addresses?
  - You might allow connections from others in the Cloud
  - Might need dynamic firewall punching
    - OGF firewalls group looking at similar problems

Issues (4)

- Best practices, minimum requirements and policies are as important as technical standards
- Are Cloud AUPs compatible with your Grid?
- If using multiple Clouds – are AUPs compatible?

Issues (5)

- Security incident response
  - A Grid site is required to inform others and participate in incident handling
  - Will the Cloud provider tell you when they have an ongoing security incident?
  - Are their systems fully patched?
  - Are there no known vulnerabilities?
  - Can we establish coordinated incident handling?
- The answer to all these is probably no!

Amazon security problem

- Security vulnerability in Amazon EC2 and SimpleDB fixed (7.5 Months after notification) (cloudsecurity.org – 18Dec08)
- AWS signature version 1 insecure
  - Man in the middle attack was possible
  - Switch to https or version 2
- Took 7.5 months to fix

Google security problem

- “Privacy group slams Google's cloud services - Search giant criticised for failing to encrypt data on servers”
  - Rosalie Marshall vnunet.com, 18 Mar 2009
- The non-profit Electronic Privacy Information Center (Epic) has filed a complaint with the US Federal Trade Commission (FTC) about the security standards of Google's cloud computing services.

Cloud Customer Agreements

- Commercial Cloud providers have lengthy legal terms and conditions
- Must be accepted to use the services
- Use Amazon as an example, but not picking on them
  - I could have used others!

Legal authority

- BY CLICKING THE “ACCEPT” BUTTON FOR THIS AGREEMENT OR ACCEPTING ANY MODIFICATION TO THIS AGREEMENT IN ACCORDANCE WITH SECTION 2 BELOW, YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE LEGAL AUTHORITY TO BIND THE LEGAL ENTITY TO THIS AGREEMENT, IN WHICH CASE “YOU” SHALL MEAN SUCH ENTITY. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT AGREE WITH THE TERMS AND CONDITIONS OF THIS AGREEMENT, YOU MUST SELECT THE “DECLINE” BUTTON AND YOU MAY NOT USE THE SERVICES.

Use by third parties outside of your organisation?

- we hereby grant you a limited, non-exclusive, non-transferable, non-sublicenseable right and license, in and under our intellectual property rights, to access and use the Services, solely in accordance with the terms and conditions of this Agreement.

Amazon EC2

- 5.4.1. Provided that you comply with the terms of this Agreement and our policies and procedures for the use of Amazon EC2, you may use Amazon EC2 to execute Applications owned or lawfully obtained by you. You are solely responsible for your Applications, including any data, text, images or content contained therein.

Amazon EC2 (2)

- 5.4.3. You are personally responsible for all Applications running on and traffic originating from the instances you initiate within Amazon EC2. As such, you should protect your authentication keys and security credentials. Actions taken using your credentials shall be deemed to be actions taken by you.

AWS Security clause

- 7.2. Security. We strive to keep Your Content secure, but cannot guarantee that we will be successful at doing so, given the nature of the Internet. Accordingly, without limitation to Section 4.3 above and Section 11.5 below, you acknowledge that you bear sole responsibility for adequate security, protection and backup of Your Content and Applications. We strongly encourage you, where available and appropriate, to (a) use encryption technology to protect Your Content from unauthorized access, (b) routinely archive Your Content, and (c) keep your Applications or any software that you use or run with our Services current with the latest security patches or updates. We will have no liability to you for any unauthorized access or use, corruption, deletion, destruction or loss of any of Your Content or Applications.

Limitations of liability

- 11.2. Applications and Content. You represent and warrant: (i) that you are solely responsible for the development, operation, and maintenance of your Application and for Your Content, including without limitation, the accuracy, security, appropriateness and completeness of Your Content and all product-related materials and descriptions; (ii) that you have the necessary rights and licenses, consents, permissions, waivers and releases to use and display your Application and Your Content; (iii) that neither your Application nor Your Content (a) violates, misappropriates or infringes any rights of us or any third party, (b) constitutes defamation, invasion of privacy or publicity, or otherwise violates any rights of any third party, or (c) is designed for use in any illegal activity or promotes illegal activities, including, without limitation, in a manner that might be libelous or defamatory or otherwise malicious, illegal or harmful to any person or entity, or discriminatory based on race, sex, religion, nationality, disability, sexual orientation, or age; (iv) that neither your Application nor Your Content contains any Harmful Components; and (v) to the extent to which you use any of the Marks, that you will conduct your business in a professional manner and in a way that reflects favorably on the goodwill and reputation of Amazon.

Indemnification

- 12.1. General. You agree to indemnify, defend and hold us, our affiliates and licensors, each of our and their business partners (including third party sellers on websites operated by or on behalf of us) and each of our and their respective employees, officers, directors and representatives, harmless from and against any and all claims, losses, damages, liabilities, judgments, penalties, fines, costs and expenses (including reasonable attorneys fees), arising out of or in connection with any claim arising out of (i) your use of the Services and/or Amazon Properties in a manner not authorized by this Agreement, and/or in violation of the applicable restrictions, AUPs, and/or applicable law, (ii) your Application, Your Content, or the combination of either with other applications, content or processes, including but not limited to any claim involving infringement or misappropriation of third-party rights and/or the use, development, design, manufacture, production, advertising, promotion and/or marketing of your Application and/or Your Content, (iii) your violation of any term or condition of this Agreement or any applicable Additional Policies, including without limitation, your representations and warranties, or (iv) you or your employees' or personnel's negligence or willful misconduct.

Final words

- Building and maintaining trust between Grid participants has been (is) difficult
- Clouds - significantly more difficult
  - Collaboration and MoU no longer work
  - Liability, indemnification etc become important
- Far from clear that we could offer services purchased by one organisation from a Cloud provider to other third parties (user, VO, …)

Links

- OGF document – Grid Security and Clouds http://forge.ogf.org/sf/go/doc15614
- Cloud Security Alliance http://www.cloudsecurityalliance.org/
- ENISA http://www.enisa.europa.eu/pages/02_03_news_2009_05_18_risk_survey.html
- Blog http://cloudsecurity.org
- AWS Security white paper http://s3.amazonaws.com/aws_blog/AWS_Security_Whitepaper_2008_09.pdf

Questions?