ENISA – Cloud Computing Security Strategy

Dr Giles Hogben

European Network and Information Security Agency (ENISA)
What is Cloud Computing?

Isn’t it just old hat?
What is cloud computing – ENISA’s understanding

- Cloud computing is not a *new technology*.
- Cloud computing is a new business model.
- It is a way of delivering computing resources.
50,000 Machines for 1 Minute
cost ~ the same as
1 machine for 1 year
What is cloud computing – ENISA’s understanding

- Near instant scalability and flexibility
- Near instantaneous provisioning
- ‘Service On demand’, usually with a ‘pay as you go’ billing system
- Programmatic management (e.g. through Web Services API)
- Highly abstracted hardware and software resources
- Shared resources (hardware, database, memory, etc...)
LOTS AND LOTS of old hat, put together with some very clever resource distribution algorithms

To make NEW Hat
Which you can rent by the hour

www.enisa.europa.eu
Which can resize (up and down) to your requirements

<table>
<thead>
<tr>
<th>Server Size</th>
<th>Disk</th>
<th>Bandwidth Limit</th>
<th>Hourly Charge</th>
</tr>
</thead>
<tbody>
<tr>
<td>512MB</td>
<td>20GB</td>
<td>20 Mps</td>
<td>$0.04</td>
</tr>
<tr>
<td>1GB</td>
<td>40GB</td>
<td>30 Mps</td>
<td>$0.08</td>
</tr>
<tr>
<td>2GB</td>
<td>80GB</td>
<td>40 Mps</td>
<td>$0.16</td>
</tr>
<tr>
<td>4GB</td>
<td>160GB</td>
<td>50 Mps</td>
<td>$0.32</td>
</tr>
<tr>
<td>8GB</td>
<td>320GB</td>
<td>60 Mps</td>
<td>$0.58</td>
</tr>
<tr>
<td>15.5GB</td>
<td>620GB</td>
<td>70 Mps</td>
<td>$1.08</td>
</tr>
</tbody>
</table>
Types of cloud
What is cloud computing – ENISA’s understanding

• Cloud computing is a new business model
  o It is a way of delivering computing resources

• Cloud computing is not a *new technology*. 
ENISA Cloud Computing Objectives

Help business and governments to gain the cost benefits of cloud computing.

While avoiding exposure to excessive NIS risks.
ENISA Deliverables and Ongoing Activities

  [http://is.gd/cem9H](http://is.gd/cem9H)
- Assurance framework 2009
- Research Recommendations 2009
- Common Assurance Maturity Model (CAMM) consortium 2010
- Gov-cloud security and resilience analysis (2010)
- 2011 (proposed) procurement and monitoring guidance for government cloud contracts.
Cloud Computing: Benefits, Risks and Recommendations for Information security
Security Benefits
Economy of Scale
Economies of scale and Security

- All kinds of security measures are cheaper when implemented on a larger scale.
  - (e.g. filtering, patch management, hardening of virtual machine instances and hypervisors, etc)
- The same amount of investment in security buys better protection.
Other benefits of scale

- **Multiple locations** by default -> redundancy and failure independence.
- **Edge networks**: content delivered or processed closer to its destination.
- **Staff specialization & experience**
  Cloud providers big enough to hire specialists in dealing with specific security threats.
Improved management of updates and defaults

- **Updates** can be rolled out much more rapidly across a homogenous platform.

- **Default VM images and software modules** can be updated with the latest patches and security settings.

- **Snapshots of virtual infrastructure (in IaaS)** to be taken regularly and compared with a security baseline.
The Risks
Very high value assets

- Most risks are not new, but they are amplified by resource concentration
  - Trustworthiness of insiders.
  - Hypervisors - hypervisor layer attacks on virtual machines are very attractive.
  - More Data in transit (Without encryption?)
  - Management interfaces – big juicy targets
Isolation failure

- Storage (e.g. Side channel attacks, see http://bit.ly/12h5Yh)
- Memory
- Virtual machines
- Resource use (e.g. Bandwidth)
RESOURCE EXHAUSTION

- Overbooking
- Underbooking

Caused by:

- Resource allocation algos
- Denial of Service
- Freak events
Key management

- Key management is (currently) the responsibility of the cloud customer.
- Key provisioning and storage is usually off-cloud.
- One key-pair per machine – doesn’t scale to multiple account holders/RBAC.
- Credential recovery sometimes available through management interface (protected by UN/PWD by).
- Copies of VM images may contain keys if not well-managed.
Key management 1

- Key storage and provisioning almost impossible to do on-cloud with current technologies
  - HSM’s don’t scale to the cloud
  - PKCS#10,11 don’t talk cloud
  - Revocation is even more complicated.
Encryption: Data must be processed in cleartext (most operations).

- Alternative 1. – HARD TO IMPLEMENT!

=> If you want to do anything useful with cloud computing, you have to trust the provider.
Data storage and processing without security guarantees?

- Alternative 2.

In the cloud provider (and their SLA) we trust...

Trust the cloud provider
Lock in

- Few tools, procedures or standard formats for data and service portability.
- Difficult to migrate from one provider to another, or to migrate data and services to or from an in-house IT environment.
- Potential dependency of service provision on a particular CP.
Loss of Governance

- The client cedes control to the Provider e.g.:
  - External pen testing not permitted.
  - Very limited logs available.
  - Usually no forensics service offered
  - No information on location/jurisdiction of data.
  - Outsource or sub-contract services to third-parties (fourth parties?)
Legal and contractual risks

- Lack of compliance with EU Data Protection Directive
  - Potentially difficult for the customer (data controller) to check the data handling practices of the provider
  - Multiple transfers of data exacerbated the problem
- Data in multiple jurisdictions, some of which may be risky..
- Subpoena and e-discovery
- Risk Allocation and limitation of liability
- Confidentiality and Non-disclosure
- Intellectual Property
Somebody else’s problem (SEP) syndrome

“Appirio Cloud Storage fully encrypts each piece of data as it passes from your computer to the Amazon S3 store. Once there, it is protected by the same strong security mechanisms that protect thousands of customers using Amazon’s services” (Thanks to Craig Balding, cloudsecurity.org for spotting this)
“YOU ARE SOLELY RESPONSIBLE FOR APPLYING APPROPRIATE SECURITY MEASURES TO YOUR DATA, INCLUDING ENCRYPTING SENSITIVE DATA.”

“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.”
Compliance Challenges

- Cloud Provider cannot provide evidence of their own compliance to the relevant requirements.
- Cloud Provider does not permit audit by the Cloud Customer.
- In certain cases, using a cloud implies certain kind of compliance cannot be achieved
Assurance Overload
Common Assurance Maturity Model (CAMM)

A minimum baseline for:

- Comparing cloud (and 3rd party) offers
- Assessing the risk to go Cloud
- Reducing audit burden or security risks
An example

- **Network architecture controls**
  - Well-defined controls are in place to mitigate DDoS (distributed denial-of-service) attacks e.g.
    - Defence in depth (traffic throttling, packet black-holing, etc..)
    - Defences are in place against ‘internal’ (originating from the cloud providers networks) attacks as well as external (originating from the Internet or customer networks) attacks.
  - Measures are specified to isolate resource usage between accounts for virtual machines, physical machines, network, storage (e.g., storage area networks), management networks and management support systems, etc.
  - The architecture supports continued operation from the cloud when the customer is separated from the service provider and vice versa (e.g., there is no critical dependency on the customer LDAP system).
2010 – CAM framework aims at provider benchmarking on security
Governments and the Cloud

- Gov Agencies and Public Organizations around the globe are moving non-critical applications towards a "cloud approach".
- Some governments (e.g. Korea) are even offering public cloud infrastructure as an innovation platform.
- In Europe we have some fast adopters, i.e. Denmark and UK, announcing/planning to move into the cloud.
Inside the G-Cloud: Whitehall’s grand cloud computing plan unveiled

Government CIO on adding SaaS to public sector IT

By Nick Heath, 28 January 2010, 12:40

NEWS An ambitious project to create a secure government cloud computing hub aiming to slash hundreds of millions of pounds from public sector IT costs has been unveiled.

Obama Administration Launches GSA Cloud Storefront Apps.gov

GSA’s USA.gov showcased as government using technology smarter, better, and faster

GSA # 10634
Government towards the Cloud: impact on service security & resilience

ENISA aims to:
✓ analyze and evaluate the impact of cloud computing on the resilience and security of GOV services.
✓ provide recommendations and good practices for European Members State planning to migrate to cloud computing.
2011 – procurement and monitoring guidelines

Procurement Criteria

CERT, ISAC

Monitoring and Supervision

www.enisa.europa.eu
Conclusions

- Cloud computing can represent an improvement in security for non-critical applications and data.
- But transparency is crucial: customers must be given a means to assess and compare provider security practices.
- Much more effort is required to achieve security levels required for higher assurance applications in the cloud.
- For once we can build security in by design, let’s not miss the chance.
Contact

Dr Giles Hogben
Secure Services Programme Manager

European Network and Information Security Agency

Giles.hogben@enisa.europa.eu
www.enisa.europa.eu