Trusted Cloud: Challenges and Opportunities

Prof. Dr. Gabi Dreö Rodosek
Chair of Communication Systems and Internet Services
E-Mail: gabi.dreo@unibw.de
Agenda

1. Cloud Computing - Status Quo
2. Trust Dilemma
3. Cloud Threat Environment
4. Trust Spectrum
5. Conclusion
Journey in the Cloud

What we see

What is there
Cloud Computing? "A question of perspective"
Multiple Choice: Cloud Computing is…
a. Web hosted and scalable applications that you can access via Browser
b. “pay-as-you-go” model (function/ duration number of users) for IT resources (storage/ compute/ software)
c. Usage of traditional PC’s, that are distributed over various locations to provide parallel processes and distributed data
d. IT Buzzword for customers– “Cutting Edge”
e. All together
Cloud Computing is ...

a. On-demand Self-Service

b. Broad Network Access: The cloud network should be accessible anywhere, by almost any device

c. Resource Pooling

d. Rapid Elasticity

e. Measured Service (QoS)
Types of Cloud services (SPI-Model)

- **SaaS** (Software as a Service)
  - Cloud User
  - Cloud Provider
  - Support
  - Provide
- **PaaS** (Platform as a Service)
  - Developers
  - Cloud Provider
  - Support
  - Provide
- **IaaS** (Infrastructure as a Service)
  - IT aaS
  - Communication aaS
  - Cloud aaS
  - Network aaS
- Abstraction
- Physical Infrastructure
Infrastructure aaS

- Highly scaled redundant and shared computing infrastructure accessible using Internet technologies

- Virtualization of the infrastructure

- Virtual server, storage, mainframes, network, telco services, VLAN’s

- Example Provider:
  - Amazon EC2, S3; EBS
  - Rackspace Mosso
  - Sun’s Cloud Services
Platform aaS
- Application aaS (1)

- Platform that enables developers to write applications that run on the cloud

- Including the management and integration of the applications

- Databases, object-oriented storage, security services, management of data

- Example Providers:
  - Microsoft Azure
  - Google App Engine
  - Amazon SimpleDB
Software aaS
- Application aaS (2)

- Access to applications
- No local installation of the application
- Everything in the hands of the provider (user data, etc.)
- Examples: Mail, CRM, Content Management, etc.
- Example Providers:
  - Google Apps
  - Salesforce.com
  - DropBox
Cloud service

Cloud API
(Soap, Rest (XML/JSON), XML-RPC, Query)

Cloud Resources

Abstraction
(Virtualization, Elasticity, Scalability)

Manage ment (FCAPS)

Cloud Provider

Cloud User

Cloud Customer

Physical Infrastructure

Cloud Service

Cloud Service

Cloud Service

Cloud Service

Cloud Service
Types of Cloud systems

- Hybrid Cloud
- Public Cloud (External)
- Media Cloud
- Logistic Cloud
- Private Cloud (Enterprise/Internal)
- Private Community
- Private Dedicated
- Cloud Broker
- Ad-hoc Cloud
- So-hosted Cloud
- Personal Cloud
- Community/ Collaborative Cloud
- Private Managed
Cloud types – Public Cloud

- = external Cloud
- Provider and user are from different organizations
- Commercial Revenue Model
- On-demand resource usage via Internet
- No (less) control and information about cloud resources
Cloud types
– Private Cloud

- = internal Cloud
- Provider and user are from the same organization
- No public access
- Private Cloud subtypes:
  - Dedicated (own organization; internal management)
  - Managed (own organization; external management)
Cloud types
– Hybrid Cloud

- Private/internal and Public/external
- Part of collaborative cloud
- Organization implements own cloud services and uses additional external cloud services
- Trade-off: cost reduction – security/data protection
Inter-Cloud Example (1)
DropBox - Amazon
Inter-Cloud Example (2)
USA – RACE and FORGE

- **App-components-as-a-service**: Google App Engine, Enasee
- **Software-platform-as-a-service**: Azure
- **Infrastructure-as-a-Service**: Amazon Elastic Compute Cloud (Amazon EC2) - Beta
- **Data Intensive**: Amazon Hadoop, Public Data Sets, Simple DB
- **Physical infrastructure**: Compute, Storage, Networking, Content Delivery
- **Hardware Resources**: GCDS Akamai
- **USA – RACE and FORGE**
Agenda

1. Cloud Computing - Status Quo
2. Trust Dilemma
3. Cloud Threat Environment
4. Trust Spectrum
5. Conclusion
Basic trust principles

1. Trust means being able to predict what other entities will do and what situations will occur.

2. Trust means making an exchange with something when you do not have full knowledge about it, its intent and the things it is offering to you.

3. Trust means giving something now with an expectation that it will be repaid, possibly in some unspecified way at some unspecified time in the future.

4. Trust means enabling other entities to take advantage of your vulnerabilities—but expecting that they will not do this.
1. Trust is comprised of security, control, service levels and compliance

2. Trust between:
   1. Cloud customer – Cloud provider
   2. Cloud provider – Cloud provider

3. Basic trust problem in the cloud:
   1. Shift data and applications to Cloud services within a Cloud provider system – „Black Box“ – no physical control/property; but still RESPONSIBILITY [EuroCloud]
   2. Easy Solution: Don‘t move to the Cloud
Dilemma of CIOs and Security Officers

1. Cloud Computing is a fact
2. Can‘t „Say no“ (technical and business advantages)
3. No Cloud Computing is not an option
4. Private Cloud is not „real“ Cloud Computing
The “Good” at Cloud Computing – just trust
Commercial Cloud formation

Amazon Elastic Compute Cloud (Amazon EC2) - Beta

TAP INTO THE POWER OF NETWORK.COM
Security questions (1)

- Who controls + manages what within the cloud?
- How do I guarantee and control my security policies along the whole lifecycle?
- How do I get my data?
- Where is my data located?
- In the event of a merger or acquisition (outsourcing, co-sourcing) will your organization inherit new compliance complications?
- Who uses the offered services? Who is liable for abuse of resources?
Security questions (2)

- Interconnection at strategic and deployable + tactical level between cloud elements
- Confidentiality? Where is ‘my’ data (in which country?), which crypto regulation rules apply, e.g. key-escrow requirements?
- Privacy? compliant with privacy legislation?
- Trustworthiness of cloud service? How does the cloud platform handle access rights, key-management, certificate management, etc.?
- Availability? Which measures against DoS, risk of data lock-in, ....
- Cloud Computing: Door opener for new kinds of attacks?
Agenda

1. Cloud Computing - Status Quo
2. Trust Dilemma
3. Cloud Threat Environment
4. Trust Spectrum
5. Conclusion
Setting the scene

1. Ubiquitous Computing
2. World-wide coallitions/partnerships/organizations
   - DISAPPEARING PERIMETER
3. Multilevel, Multi-community Security Domains
   - COLLABORATION
4. Multiple requirements for services + information
5. Cyber Threat
Security challenges, implications

- Abuse of Cloud Computing Resources
- Shared Technology Vulnerabilities
- Data Loss Leakage
- Insecure Application Programmer Interface
- Account, Service & Traffic Hijacking
- Malicious Insiders
- Unknown risk profile
- Some threats in more detail
1. Abuse of Cloud Computing Resources
   • Problem: “unlimited” usage of cloud resources – anonymous users (DoS, password cracking, botnets, etc.)
   • Controls: registration + validation of the user, control of network traffic

2. Shared Technology Vulnerabilities
   • Problem: provider use same physical infrastructure for many customers (cash, storage), deficits in isolation concepts – information leak, illegal access
   • Controls: access control, monitoring of activities, vulnerability scans and audit
3. Data Loss Leakage

- Problem: missing backup concepts, deficit access control, loss of keys, missing audits
- Controls: access control (multi factor), redundancy + backups, encryption and key management

- Insecure APIs
  - Problem: deficit security concepts for API’s (authentication, encryption, logging, access control), multi-hop usage of APIs (plaintext passwords, reuse of security tokens)
  - Controls: security analysis (risk management) and sufficient security controls within an coherent security concept
Cloud Computing attacks

<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>Reported</th>
<th>Summary</th>
<th>Organization</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>508</td>
<td>outage</td>
<td>2011-04-21</td>
<td>Companies left staggering or totally knocked out because of server problems in the Amazon datacenter</td>
<td>Amazon Web Services</td>
<td>Amazon Elastic Compute Cloud (Amazon EC2)</td>
</tr>
<tr>
<td>509</td>
<td>outage</td>
<td>2011-04-21</td>
<td>PlayStation Network outages</td>
<td>Sony</td>
<td>PlayStation Network</td>
</tr>
<tr>
<td>495</td>
<td>outage</td>
<td>2011-03-25</td>
<td>Twitter Experiences Delays in Delivering to Facebook and SMS</td>
<td>Twitter, Inc.</td>
<td>Twitter</td>
</tr>
<tr>
<td>496</td>
<td>outage</td>
<td>2011-03-25</td>
<td>Heroku Users Experience HTTP 503 Errors</td>
<td>Heroku</td>
<td>Cloud Hosting</td>
</tr>
<tr>
<td>497</td>
<td>outage</td>
<td>2011-03-25</td>
<td>Twitter Experiences Tweet Delivery Delay</td>
<td>Twitter, Inc.</td>
<td>Twitter</td>
</tr>
<tr>
<td>498</td>
<td>outage</td>
<td>2011-03-25</td>
<td>Heroku Shared Database Experienced Hardware Failure</td>
<td>Heroku</td>
<td>Cloud Hosting</td>
</tr>
<tr>
<td>499</td>
<td>outage</td>
<td>2011-03-25</td>
<td>Heroku Users Unable to Provision New Dedicated Databases</td>
<td>Heroku</td>
<td>Cloud Hosting</td>
</tr>
<tr>
<td>500</td>
<td>hack</td>
<td>2011-03-24</td>
<td>TripAdvisor Member Data Stolen in Possible SQL Injection Attack</td>
<td>Expedia</td>
<td>TripAdvisor</td>
</tr>
<tr>
<td>501</td>
<td>outage</td>
<td>2011-03-23</td>
<td>Netflix Streaming and Web Site Down</td>
<td>Netflix</td>
<td>Netflix Streaming</td>
</tr>
<tr>
<td>488</td>
<td>outage</td>
<td>2011-03-21</td>
<td>Heroku New Relic Deployment Notification Outage</td>
<td>Heroku</td>
<td>Cloud Hosting</td>
</tr>
</tbody>
</table>

“Cloutage”:
- 505 incidents
- 396 Outage
- 71 Vulnerabilities
- 40 Autofail
- 21 Hack
- 4 Dataloss

http://cloutage.org/incidents
Example of an attack

• Virtualization
  • Vulnerable VM Monitor: access to all data

• Attack scenario:
  • Distribution of VM Images via “Public Market Places”
  • Amazon Machine Image (AMI) market place for EC2: “AMIs are launched at the user's own risk. Amazon cannot vouch for the integrity or security of AMIs shared by other users. […] Ideally, you should get the AMI ID from a trusted source […].”
  • Attack: Setup of botnets, data leakage,…
„Dropbox employees are prohibited from viewing the content of files you store in your Dropbox account, and are only permitted to view file metadata (e.g., file names and locations). Like most online services, we have a small number of employees who must be able to access user data for the reasons stated in our privacy policy (e.g., when legally required to do so). But that’s the rare exception, not the rule. We have strict policy and technical access controls that prohibit employee access except in these rare circumstances. In addition, we employ a number of physical and electronic security measures to protect user information from unauthorized access.“ – „Patriot Act“
Agenda

1. Cloud Computing - Status Quo
2. Trust Dilemma
3. Cloud Threat Environment
4. Trust Spectrum
5. Conclusion
Spectrum trust

Reference Architecture
Customer Reviews (StratusLab)
Risk Analysis (ENISA)

Security Objectives
Law/Regulation (PCI, SOX, HIPAA)
Standards/Guidance

Internal Information
Globale Security Startegy of Organization
specified in

Risk Management (Lifecycle)

Security Requirements
translated in

Security Controls

Cloud Resources
relate to

Security Concept
describes implementation

protect
Spectrum trust

1. Risk assessment cloud customer
2. Security controls of the cloud provider → Security requirements of the cloud customer
   1. General requirements (compliance, certification, etc.)
   2. Operative requirements (transport encryption, data location, etc.)
3. Confirm implementation of security controls within SLAs
4. Controls of Trust (to get „belief information“)
Security controls (trade-off)

1. General: Cloud provider’s responsibility to assure security according cloud customers requirements

2. Trade-off:
   1. SaaS: most integrated security functionality built directly into the offering, with the least consumer extensibility
   2. PaaS: security features and capabilities, where the builtin capabilities are less complete, but there is more flexibility to layer on additional security
   3. IaaS: less integrated security capabilities and functionality beyond protecting the infrastructure itself → requires that OS, applications, and content are be managed and secured by the cloud customer
Security controls (trade-off)
# Spectrum Cloud Security Mechanisms

<table>
<thead>
<tr>
<th>People and Identity</th>
<th>Data and Information</th>
<th>Application and Process</th>
<th>Network, Server, and Endpoint</th>
<th>Physical Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged User Access</td>
<td>Data Segregation</td>
<td>Compliance and Auditing</td>
<td>Server Security</td>
<td>Data Location</td>
</tr>
<tr>
<td>Federated Identity Management</td>
<td>Data Recovery</td>
<td>Investigative Support</td>
<td>Network Security</td>
<td>Disaster Recovery</td>
</tr>
<tr>
<td>Privileged Account Management</td>
<td>Data Redaction and Termination</td>
<td>Policy Management</td>
<td>Virtualization Security</td>
<td>Cloud Availability</td>
</tr>
<tr>
<td></td>
<td>Data Leakage Prevention</td>
<td>Secure Provisioning</td>
<td>Browser Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Application Testing</td>
<td>Patch Management</td>
<td></td>
</tr>
</tbody>
</table>

- **End User**
- **Enterprise Administrator**
- **IT Auditor**
- **Application Developer**
- **Cloud Provider**
Spectrum
security SLOs within SLAs

1. Related to security services and mechanisms
2. Related to security management processes (incident, vulnerability assessment, penetration tests)
3. Overall compliance of the cloud provider (HIPPA, SOX)
4. Certification/accreditation (ISO 20000/2700x, Common Criteria, SAS 70)
5. Related to cloud service location (region, no sub-providers, dedicated physical resources)
Controls of trust

1. Cloud provider – Cloud customer (direct trust)
   1. Security concepts
   2. Audit reports from the cloud provider

2. Control through „implicit“ third party (certification/ accreditation) (indirect trust)

3. Control through third party (indirect trust)
   1. Cloud Trust Broker
   2. Trust mechanisms (Cloud Trust Protocol, PKI, Federated Identity Management)
Controls of trust (1)
security concepts
Controls of trust (2)
certification/accreditation

1. Example: „Amazon Web Services: Risk and Compliance“
   1. SAS70 Type II: independent auditor report about effective operation of security controls (No public access to the report)
   2. PCI DSS Level 1: AWS comply with the PCI Data Security Standard as a shared host service provider
   4. FISMA: AWS approval to operate at the FISMA-Low level + passed the independent security testing and evaluation required to operate at the FISMA-Moderate level
Controls of Trust (3)

Cloud Trust Protocol

1. Trusted Cloud Service decision support
   - Trusted cloud services business needs analysis and recommendations (CloudAssist)

2. Orchestrator of Orchestrators
   - The automated arrangement, coordination, connection, and accountability for individual cloud service contributions

Business and technical needs integration knowledge

CloudTrust Protocol (with SCAP)

Service interfaces:
- Google
- Terremark
- CSC Trusted Cloud
- Private Cloud
- Amazon
- Microsoft
Final trust conclusion

1. Identify your trust perspective (provider vs. customer)
2. Do you all trust that controls? – need of organization specific risk management
   1. Identify application and data sets that can be moved to the Cloud
   2. Identify threats and vulnerabilities
   3. Define security controls
   4. Market analysis of provider offerings
   5. Negotiate security related SLOs within SLA
   6. CONTROL!
Nothing is for free!
(Especially for Security&Trust)