Cloud Security 2011

Prof. Dr. Michael Waidner
Fraunhofer SIT
Security and Privacy »made in Darmstadt«

CASED
Center for Advanced Security Research Darmstadt

170 employees, 70 full-time researchers, 2 TU professors

Fraunhofer
SIT

10 professors, incl. 6 chairs, with strong security focus

15 professors with more than 100 researchers in CASED

6 professors
Outline

1. Cloud Computing
2. Security and Privacy Challenges
3. Trusted Cloud

Acknowledgement: These slides are partially based on a presentation prepared for IBM.
Outline

1. Cloud Computing
2. Security and Privacy Challenges
3. Trusted Cloud
**Consumption and Delivery Model for IT Services**

*“Cloud” represents the industrialization of delivery for IT supported services*

<table>
<thead>
<tr>
<th>Deployment Models</th>
<th>Private Cloud</th>
<th>On Premise</th>
<th>Community Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Cloud</td>
<td>Off Premise</td>
<td>3rd-Party Managed</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service Models</th>
<th>Business Process as a Service (BPaaS)</th>
<th>Software as a Service (SaaS)</th>
<th>Platform as a Service (PaaS)</th>
<th>Infrastructure as a Service (IaaS)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Essential Characteristics</th>
<th>On Demand Self-Service</th>
<th>Broad Network Access</th>
<th>Resource Pooling</th>
<th>Rapid Elasticity</th>
<th>Measured Service</th>
<th>Service Mgmt</th>
<th>Automation</th>
</tr>
</thead>
</table>

|------------------------|---------------|-------------------------|------------------|---------------------|------------------------|------------------|--------------|-----------------------|---------------------|

<table>
<thead>
<tr>
<th>Cloud Enables</th>
<th>Economies of scale</th>
<th>Sourcing Options</th>
<th>Flexible payment models</th>
</tr>
</thead>
</table>

Adapted from: [Mell, Grance: The NIST Definition of Cloud Computing; NIST SPUB 800-145]
## Why Cloud Computing?

### Results from IBM cloud computing engagements

<table>
<thead>
<tr>
<th>Increasing speed and flexibility</th>
<th>Test provisioning</th>
<th>Weeks</th>
<th>Minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change management</td>
<td></td>
<td>Months</td>
<td>Days/hours</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Weeks</td>
<td>Minutes</td>
</tr>
<tr>
<td>Release management</td>
<td></td>
<td>Administered</td>
<td>Self-service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Complex</td>
<td>Reuse/share</td>
</tr>
<tr>
<td>Service access</td>
<td></td>
<td>Fixed cost</td>
<td>Variable cost</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10–20%</td>
<td>70–90%</td>
</tr>
<tr>
<td>Standardization</td>
<td></td>
<td>10–20%</td>
<td>70–90%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Years</td>
<td>Months</td>
</tr>
</tbody>
</table>

© IBM, 2010
Moving from Private to Public Leads to a Real or Perceived Loss of Control

We Have Control
- It's located at X.
- We have backups.
- Our admins control access.
- Our uptime is sufficient.
- The auditors are happy.
- Our security team is engaged.

Who Has Control?
- Where is it located?
- Who backs it up?
- Who has access?
- How resilient is it?
- How do auditors observe?
- How does our security team engage?

33%
Of respondents are concerned with cloud interfering with their ability to comply with regulations

80%
Of enterprises consider security #1 inhibitor to cloud adoptions

48%
Of enterprises are concerned about the reliability of clouds

Source: Driving Profitable Growth Through Cloud Computing, IBM Study, 2008 (conducted by Oliver Wyman)
Enterprises Significantly Prefer Private over Public

Overall, how appealing are the public, private and hybrid delivery models for your company?

- Private: 64%
- Hybrid: 38%
- Public: 30%

Public vs. Private trade-off considerations

Benefits
- Increased Speed
- Lower Cost

Security
- Insecure or incomplete data deletion
- Isolation failure
- Malicious Insiders
- Management infrastructure compromise

Governance
- Resiliency
- Level and source of support
- Architectural & management control
- Compliance

Customization / specialization

Source: IBM Market Insights, Cloud Computing Research, July 2009. n=1,090
Cloud Service Model Suggests Split of Responsibilities between the Provider of Public Clouds and the Subscribers

Who is responsible for security at the ... level?

<table>
<thead>
<tr>
<th>Datacenter Infrastructure</th>
<th>Middleware</th>
<th>Application</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider</td>
<td>Subscriber</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provider</td>
<td>Subscriber</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provider</td>
<td>Subscriber</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Provider/Subscriber service agreement determines actual responsibilities.
Workloads may be at Different Levels of Cloud Readiness

- Ready for Cloud
- Analytics
- Infrastructure Storage
- Industry Applications
- Collaboration
- Workplace, Desktop & Devices
- Business Processes
- Disaster Recovery
- Development & Test
- Infrastructure Compute

Collaborative Care
- Medical Imaging
- Financial Risk
- Energy Management

Information intensive
- Isolated workloads
- Mature workloads

Sensitive Data
- Highly customized
- Not yet virtualized 3rd party SW
- Complex processes & transactions
- Batch processing

Market bias:
- Private cloud
- Public cloud

New workloads made possible by clouds ...

Market bias:
- Private cloud
- Public cloud

© IBM, 2010
Outline

1. Cloud Computing
2. Security and Privacy Challenges
3. Trusted Cloud
What is Cloud Security?

Confidentiality, integrity, availability of business-critical IT assets
Stored or processed on a cloud platform

There is nothing new under the sun but there are lots of old things we don't know.

Ambrose Bierce, The Devil's Dictionary
Data are Central to the Analysis of Risks and Threats

*CSA (2010), ENISA (2009), Gartner (2008), IBM X-Force (2010), ...*

<table>
<thead>
<tr>
<th>Transformation</th>
<th>1. Vendor lock-in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy and Data</td>
<td>2. Data security</td>
</tr>
<tr>
<td>Data Compliance</td>
<td>3. Data protection, meeting privacy needs and expectations</td>
</tr>
<tr>
<td></td>
<td>4. General and industry-specific compliance</td>
</tr>
<tr>
<td></td>
<td>5. Uncertainty over data location</td>
</tr>
<tr>
<td></td>
<td>6. Inability to respond to law enforcement requests</td>
</tr>
<tr>
<td>Data Recovery</td>
<td>7. Data recovery, resiliency</td>
</tr>
<tr>
<td>Classical IT Security</td>
<td>8. Account or service hijacking</td>
</tr>
<tr>
<td></td>
<td>9. Insecure interfaces and APIs</td>
</tr>
<tr>
<td></td>
<td>10. Management (incl. self-service) interface compromise</td>
</tr>
<tr>
<td>Shared IT</td>
<td>11. Insecure or incomplete data deletion</td>
</tr>
<tr>
<td></td>
<td>12. Process/VM isolation, data segregation, multi-tenancy</td>
</tr>
<tr>
<td></td>
<td>13. Malicious insiders (co-tenants, cloud provider)</td>
</tr>
<tr>
<td></td>
<td>14. Abuse of cloud services (extrusion)</td>
</tr>
</tbody>
</table>
Two Parallel Trends: Mobile Access to Cloud-delivered Services

Cloud model suggests and supports ubiquitous access via resource constrained and often personally owned devices

- Mobile access and public cloud both blur the enterprise perimeter
- New endpoints (e.g., iOS, Android) with new security characteristics and challenges,
- Often used for personal and business purposes
- “Bring your own device”: Consumerization of IT often collides with enterprise security principles
Cloud Users often do not Understand Cloud Characteristics

Fraunhofer SIT Analysis of 1100 Public Amazon Machine Images, Spring 2011

About 1/3 with major vulnerabilities

- Caches, shadow files, ...
- Passwords
- Public SSH keys
- Private SSH keys
Components of a Cloud Security Solution

- Isolation
- Identity
- Compliance
- Trust
Isolation – Software, Server, Network
Coloring/Labeling Resources, Events, …

- **State of the art**
  - Service and Application
    - Can be done at all levels of the stack
  - Server
    - Hypervisor: z/VM, LPAR, pHype, Xen, VMware ESX, ...
  - Network
    - Security Zones, Trusted Virtual Domains
    - VLAN (IEEE 802.1Q)
    - Trusted / Secure Virtual Private Networks (VPN)
    - Encryption of data in transit (SSL/TLS, SSH, IPSec)

- **Key Issues**
  - Standardized policies
  - Verification of isolation
  - Application security → VM security
  - Network security → VN security
Isolation – Data, Storage, Backups
Coloring/Labeling Resources, Events, ...

- State of the art
  - Label-based Access Control (LBAC)
  - Storage zoning (Virtual Storage Area Network, ...)
  - Enforcing location (per privacy laws)
  - Cleanup of caches, files, disks, backups, ...
  - Encryption of data at rest
    - Data deduplication vs. encryption
    - Provider vs. individual keys
    - In-cloud vs. extra-cloud key management
  - Fully homomorphic encryption

- Key Issues
  - Standardized policies
  - Standardized data portability
  - Meaningful key management
  - Research in advanced crypto
Identity
Main types of identities to consider in a cloud

- **Standard identity management + access/usage control**
  - Major risk: reinventing the wheel ...
  - Major challenge: correlation of of identities and security events across multiple layers in the cloud stack

- **Cloud subscriber administrators**
  - Initial enrollment and proofing of cloud subscriber
  - Trust depends largely on proofing of identities
    - Valid email address
    - Upfront payment
    - Out-of-band signed service contract

- **Cloud subscriber end user identities**
  - Subscriber's employees, customers, ...
  - Efficient on-boarding / off-boarding
  - Directory synchronization (bad idea)
  - Federated identity (good idea, standard in SOA)

- **Cloud provider administrators**
  - Major issue: Control over privileged identities
Compliance
Meeting Regulatory Requirements

- Provider auditing
- Subscriber-level auditing
  - Practically often very hard
- Privacy
  - Data encryption and suitable key management
  - Enforcing data location
  - Prevent cross-border data flows
- Cloud Forensics
  - Discover evidence related to a specific cloud subscriber
  - Freezing and surrendering virtual resources
  - Protect confidentiality of third parties resources
Good candidates for security-as-a-service are functions which

- Can be delivered without on-premises technology
- Latency-tolerant
- Require minimal customization
- Involves one-to-many data management or analysis functions
- Can be implemented though standard interfaces
- Unlike managed security services, not labor-intensive

<table>
<thead>
<tr>
<th>Function</th>
<th>Now</th>
<th>2013</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messaging / Email Security</td>
<td>20%</td>
<td>60%</td>
<td>70%</td>
</tr>
<tr>
<td>Secure Web Gateway</td>
<td>10%</td>
<td>35%</td>
<td>65%</td>
</tr>
<tr>
<td>Remote Vulnerability Scanning</td>
<td>10%</td>
<td>30%</td>
<td>45%</td>
</tr>
<tr>
<td>Security Information and Log Management</td>
<td>1%</td>
<td>10%</td>
<td>25%</td>
</tr>
<tr>
<td>Identity &amp; Access Management</td>
<td>2%</td>
<td>20%</td>
<td>28%</td>
</tr>
<tr>
<td>Security Intelligence</td>
<td>60%</td>
<td>80%</td>
<td>85%</td>
</tr>
</tbody>
</table>

Source: Kelly Kavanagh, Gartner Research
In-Security as a Service

Zeus botnet finds hold in Amazon cloud
Published: 2009-12-11

The cybercriminals behind the Zeus botnet used Amazon's Elastic Computing Cloud (EC2) to host the central server used to control a portion of the compromised machines, security firm CA stated on Thursday.

Cybercrime-as-a-service takes off

Malware writers that sell toolkits online for as little as $400 will now configure and host the attacks as a service for another $50, a security expert has said.

Roger's Security Blog

As Chief Security Advisor of Microsoft EMEA - lets share interesting security information

Cybercrime as a Service—Our Future?

It is not really surprising that the criminals will leverage the economy of Cloud Computing for their illegal purposes. Especially activities, which consume a lot of processor power will be moved to the Cloud — like any other business.
Outline

1. Cloud Computing
2. Security and Privacy Challenges
3. Trusted Cloud
Trusted Cloud – Why?

- What trust is needed?
  - Varies by market segment, workload, type of data
  - Different answers for governments, regulated industries, “regular” enterprises, private users, etc.

- Business opportunity “Trusted Cloud”

- Success of the cloud model: Perceived benefits dominate stated security and privacy concerns

- Cloud users are taking more risk than they feel comfortable with
  - Market very sensitive to real or perceived cloud security incidents
Trusted Cloud – How?

• Trust by *Competence*
  • Better security through well managed public clouds

• Trust by *Technology*
  • State-of-the-art security & privacy processes and technology
  • But: cloud inherits all security problems of enterprise computing (+ some new …)

• Trust by *Certification*
  • Who audits and certifies against what standard? International audits?

• Trust by *Agreement*
  • Service-level agreements may offer adequate security, privacy and transparency
  • What are the minimum standards for cloud security and privacy?
  • *Cloud SLA:* standardized and cheap –
    *Outsourcing SLA:* customized and expensive

• Trust by *Enforcement*
  • Is there market demand for Trusted Computing concepts?
Prof. Dr. Michael Waidner  
michael.waidner@sit.fraunhofer.de

Fraunhofer-Institute for  
Secure Information Technology  
Rheinstrasse 75  
64295 Darmstadt, Germany  
www.fraunhofer.de  
www.sit.fraunhofer.de

Technical University of Darmstadt  
Chair for Security in Information Technology  
Mornewegstrasse 30  
64289 Darmstadt, Germany  
www.cased.de  
www.sit.tu-darmstadt.de