

Technische Herausforderungen der Cloud-Forensik



Dominik Birk

Horst Görtz Institute for IT Security
Bochum (Germany)

Anwendertag IT-Forensik 2011

April 12th, 2011, Darmstadt

The Speaker



Dominik Birk

- Ph.D. Student at the Horst Görtz Institute for IT Security (HGI)
- Focus: Cloud Security & Forensics

- Freelancer in the Field of IT Security

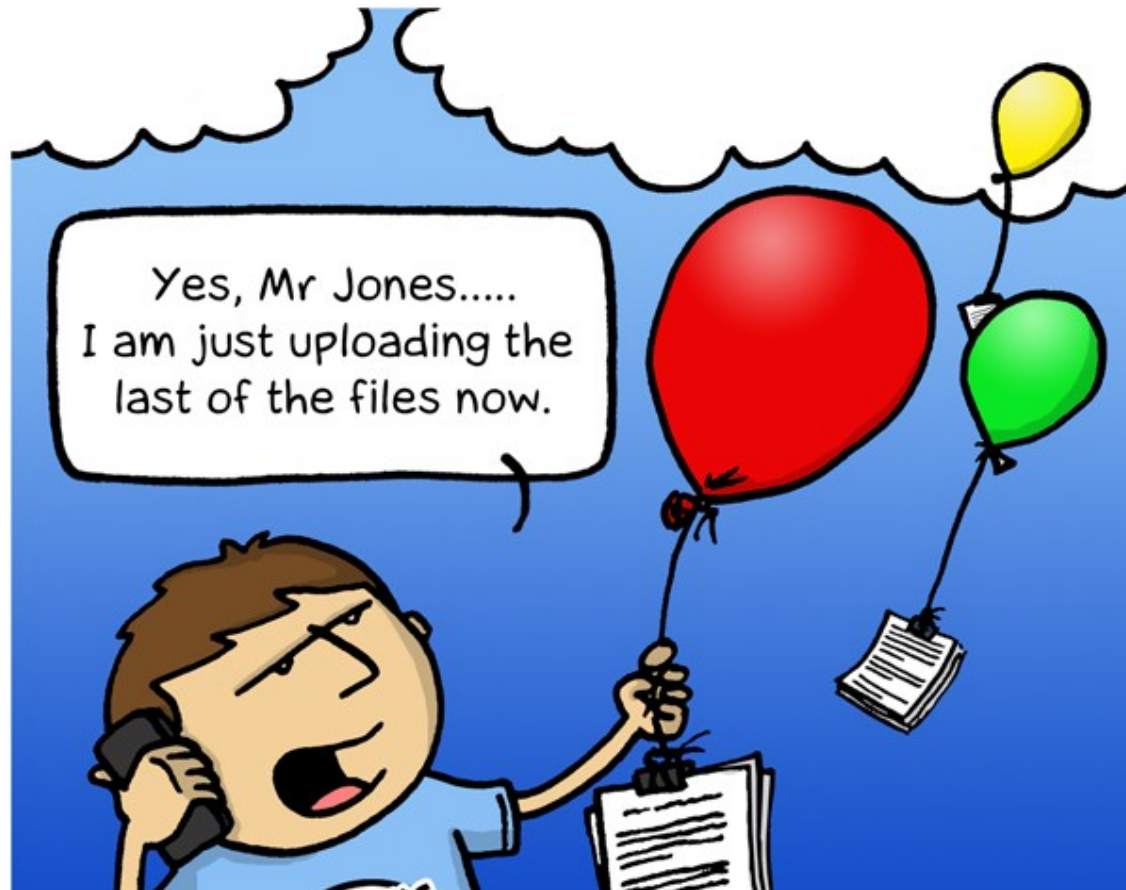


Dr. Christoph Wegener, CISA, CISM

- Horst Görtz Institute for IT Security (HGI)
- Freelancer (wecon.it-consulting)
- Member of a-i3, GUUG, ISACA

- Main interests: Cloud Security, Network Security, Security and Privacy Issues in Social Networks

Cloud Computing – Make it Run!



Cloud Computing – Make it Secure!



Cloud Computing – Make it Secure?



What happens if Security fails?








Do You Know Where Your Data is in the Cloud?

Most Restrictive	Restrictive	Some Restrictions	Minimal restrictions	Pending Legislation
Argentina	Ireland	Estonia	Hong Kong	Turkey
Germany	Netherlands	Hungary	India	Malaysia
Switzerland	Norway	Iceland	US	Mexico
	Austria	Slovakia	Australia	Brazil
	Belgium	South Korea	Colombia	China
	Bulgaria	Canada	Russian Federation	Singapore
	Cyprus	Czech Republic	Taiwan	Thailand
	Denmark	Israel	Chile	
	Finland	New Zealand	Japan	
	France		South Africa	
	Greece		Paraguay	
	Italy			
	Latvia			
	Lithuania			
	Luxembourg			
	Poland			
	Portugal			
	Slovenia			
	Spain			
	Sweden			
	UK			

Source: <http://www.forrester.com/cloudprivacyheatmap>



Scuse'me, why should I bother?

	2009 2011	<ul style="list-style-type: none">- unauthorized access to GoogleDocs- Gmail data loss- Gmail Outage
	2008 2009	<ul style="list-style-type: none">- silent data corruption in S3- S3 outage
	2010	<ul style="list-style-type: none">- compromisation of account information, including payment card data
	2009	<ul style="list-style-type: none">- Microsoft Hotmail downtime- Microsoft Azure outage
	2008 2009 2010	<ul style="list-style-type: none">- unencrypted external storage device- service outage- employee was tricked by Phishing Attack

Amazon Web Services™ Customer Agreement

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.**

[...]

you acknowledge that you bear sole responsibility for adequate security, protection and backup of Your Content. We strongly encourage you, where available and appropriate, to use encryption technology to protect Your Content from unauthorized access and to routinely archive Your Content. **We will have no liability** to you for **any unauthorized access or use, corruption, deletion, destruction or loss** of any of Your Content.

Fault Model

- Data and information in the cloud can be affected by inconsistencies
- **Maliciously Intended Faults:**
Internal or external adversaries, economic rivals, former employees, malicious CSP
- **Unintentional Faults:**
Internal communication errors, human failures, ...



Tell me, why is the Cloud so dark?

- Cloud Service Provider (CSP) artificially eclipse the Cloud for several reasons:
 - Competitors could use workload information for improving their own range of services or use it to harm the reputation of the CSP.
 - Adversaries could use technical information about infrastructure and system usage for launching attacks against the provider.
- Additionally, this "darkness" lies in the current principle of flexibility in the field of Cloud Computing.
- These circumstances yield one main issue: *Is it possible for the customer to perform a traditional digital investigation in case it is needed for one of his virtual instances in the cloud environment of the vendor and if so, where the investigation begins?*

SAP Cycle

Conventional Digital Forensics

- "*Chain of Custody*" is needed
- The **Securing-Analyzing-Presentation** (SAP) Cycle
 - Digital Investigations require an appropriate **Securing** of evidence data. This normally happens with the help of bitwise duplication of the physical volume.
 - During the **Analyzing** stage, bits and pieces are pulled together for *deciphering* the story of what happened.
 - In the **Presentation** phase, all other phases are documented and explained.

Digital Forensics in Real Private Clouds

- **Securing the data:** Possible because the *Cloud* is in your own data center ✓
- **Analyzing:** Possible because you have trustworthy access-logs, images of VMs, router logs etc ... ✓
- **Problem:**
 - Private Clouds do not offer the advantages of real Public Clouds and scale only for huge companies with the help of extraordinary investments → Security vs. Business.



Digital Forensics in Real Public Clouds

- **Securing the data:** You cannot secure the data in the traditional way because you don't know where exactly it is. ✘
- **Analyzing:** You possibly don't have trustworthy access-logs, images of VMs, router logs etc ... ✘
- **Problem:**
 - Public Clouds do offer a lot of advantages, however they represent a risk to your sensitive data.
 - The absence of physical access leads to further problems especially in cases of digital investigations.

Forensics in SaaS

- Eventually high-level logs will provide information
- Highly depends on what the CSP logs
- No deeper view into the system and its underlying infrastructure is possible
→ connection through API only
- No possibility to install any toolkits, analysis tools etc.



Source: startswithabang.com

- *"Srsly, You know nothing about your data in SaaS environments"*

hg i

Horst-Görtz Institut
für IT Sicherheit

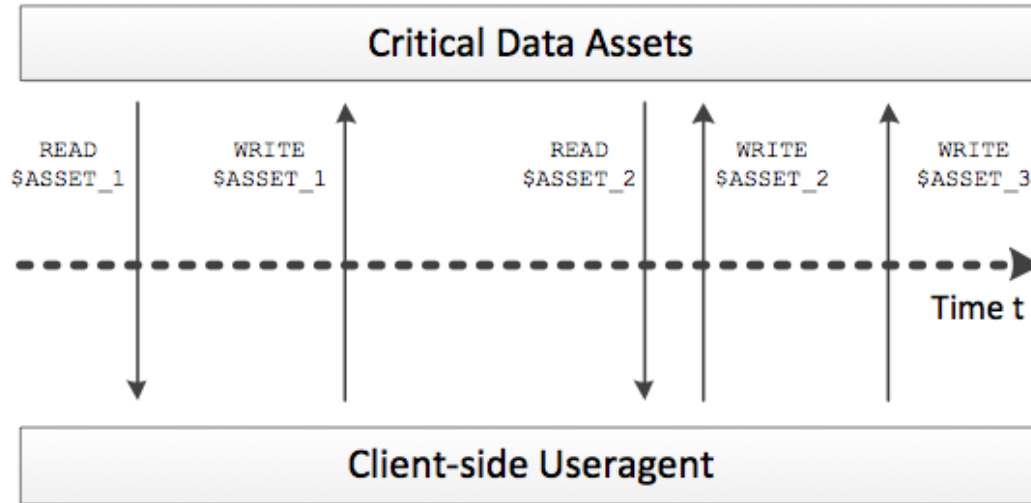
Potential Solutions?

- CSP should provide meaningful high-level logs to their customers
- Evidence data could be offered to the customers through a forensic API:
 - Data Provenance through access, error and event logs
 - *“Who accessed my email on GMail at what time?”*
- Use already established Web Application Forensics Methodologies



Data Provenance for Forensics in SaaS Cloud Environments

- Data Provenance: “ ... known as meta-data that describes the ancestry or history of digital objects.” *
- A time series of logged READ and WRITE access events within a given time-frame can be used to provide data provenance



* K. Muniswamy-Reddy and M. Seltzer, *Provenance as First Class Cloud Data*



Forensics in PaaS

- You can control your own source!
- No control over the environment where the application runs
- **Problem:** Even if you log syscalls of your application, the underlying runtime environment can modify it.
- Again, what you get depends strongly on the CSP



Source: DPA

Potential Solutions?

- Customers should never trust the features offered by the CSP
 - Example: Encrypt your data on your own instead of relying on the encryption offered by PaaS CSP
- Establish application logging on your own
 - Sign and encrypt your log-data on the fly before transferring it to third party servers for analysis



Forensics in IaaS

- Complete control over the VM – but not the host system!
- It's possible to install suitable tools and configure your system for forensic purposes.
- What happens if you turn off the VM or cancel the contract?
- You still don't know the exact location of your data!

Interesting: <http://blog.cloud404.com/2010/01/22/cloud-investigation-%E2%80%93-part-deux/>



Horst-Görtz Institut
für IT Sicherheit

Potential Solutions?

- Prepare your VMs for forensic investigations
- Make use of the power of snapshots for forensics
- Current Research:
 - Combine VM-specific guest system logs with evidence data provided through the hypervisor (*virtual introspection*) → only in collaboration with the CSP who controls the hypervisor

Interesting: "Forensics Examination of Volatile System Data Using Virtual Introspection" Brian Hay et al

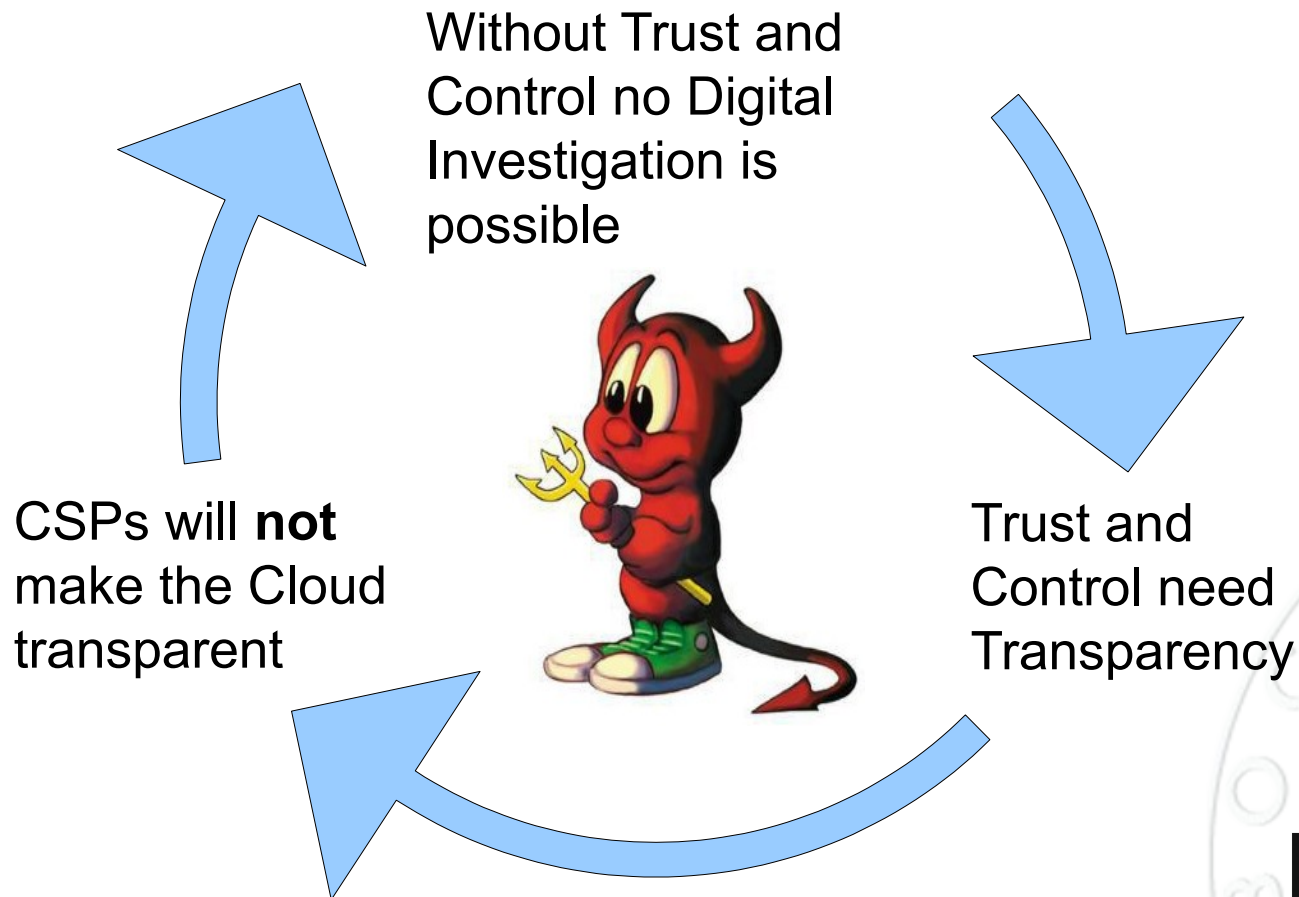


Summary: Cross-Disciplinary Aspects

- Lack of Transparency
- Loss of Evidence Data
- Compliance Issues
- Secure Data Deletion
- SLA Verification
- Missing Best Practices



Future Problem of Cloud Forensics



See: *Digital Trust in the Cloud - Liquid Security in Cloudy Places*

Conclusion

- The CSP obtains all the power!
 - If you cannot trust the CSP, leave the Cloud!
- Methods of digital forensics have to be revised and adapted to the new Cloud Computing environment
 - Will digital images (snapshots) be trusted by courts?
- CSPs should think about ...
 - ... giving the investigators the option of reconstructing the corresponding environment for recreating scenarios and test hypotheses.
 - ... offering customers physical hosts for solely usage.



Thanks for Your Attention!



Dominik Birk
dominik.birk@rub.de

