

Forensics 2.0: Challenges in the Cloud

Dominik Birk, and Dr. Christoph Wegener
Horst Görtz Institute for IT Security
Bochum (Germany)

Trust 2010 - Workshop on Trust in the Cloud
Juni 22nd, 2010, Berlin



The Speaker



Dominik Birk

- Horst Görtz Institute for IT Security (HGI)
- Freelancer

- Main interests: Cloud & Browser Forensics, Security and Privacy Issues in Social Networks, Web 2.0 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

What's this all about?

- Dr. Andy Jones (Head of Security Research at BT) outlined the following emerging **challenges in the field of digital investigations** at the *e-Forensics 2009* in Australia:

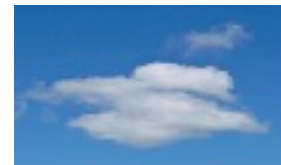
- Impact of solid-state memory



- Ultra-portable devices



- Distributed storage
also known as **Cloud Computing**



Scuse'me, why should I bother?

- In "*Assessing the Security Risks of Cloud Computing*" Gartner specifically highlighted the investigative support and auditing within Cloud Computing environments ...
- "[...] to our knowledge, no research has been published on how cloud computing environments affect digital artifacts, and on acquisition logistics and legal issues related to cloud computing environments"
Digital Forensic Research: The Good, the Bad and the Unaddressed – Bebee, Nicole
- Safe Harbor agreement vs. USA Patriot Act
Who will win the prioritization race in front of a court?
- *Scuse'me, do **You** know where your data is in the Cloud?*

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.

Cloud Computing Deployment Models

ISACA Definition

- Private
 - Operated solely for an organization
 - May not provide the scalability and agility of public cloud services
 - Community
 - Shared by several organizations
 - Public
 - Made available to the general public
 - Owned by an organization selling cloud services (CSP)
 - Hybrid
 - Composition of public and private clouds bound together by standardized or proprietary technology
-



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.

Example: AWS Virtual Private Cloud (VPC)

- **Guessing Game:** Is Amazon's VPC a real *Private Cloud*?
 - VPC principle: Put your EC2 instances in one VLAN cluster with IPsec VPN connection to your company network at home
- **Question:** Do your EC2 instances still share one physical host with other potentially evil instances?
See: Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds
- Traditional forensic investigations are still **not** possible.
- **Advantage:** The VPC is still a real Cloud with all its pros and cons.

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

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

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/>

Solving the Problem

Forensics on Guest Systems

- Possibility to create Snapshots, made by the system, not by the digital investigators
 - Do these Snapshots get admitted in court?
- Even if guest system is shut down, system memory is still there
 - Nice place for forensic investigations
 - But this depends on the VMM and postulates access to the host system
- **Conclusion:**
 - Basic approaches on digital investigations are possible, but you, and the court, have to trust the CSP.
 - Why should the CSP manipulate digital evidence?



Solving the Problem

Forensics on Host Systems

- Firewall logs could be of interest ...
 - Neighbor-2-neighbor attacks
 - Network attacks in general
- System logs could be of interest ...
 - VMM: Privilege Escalation, Memory Corruption, ...
 - Covert channel attacks?
- But even if you have control over the host system, you have to trust the CSP
 - You still don't control the hardware!



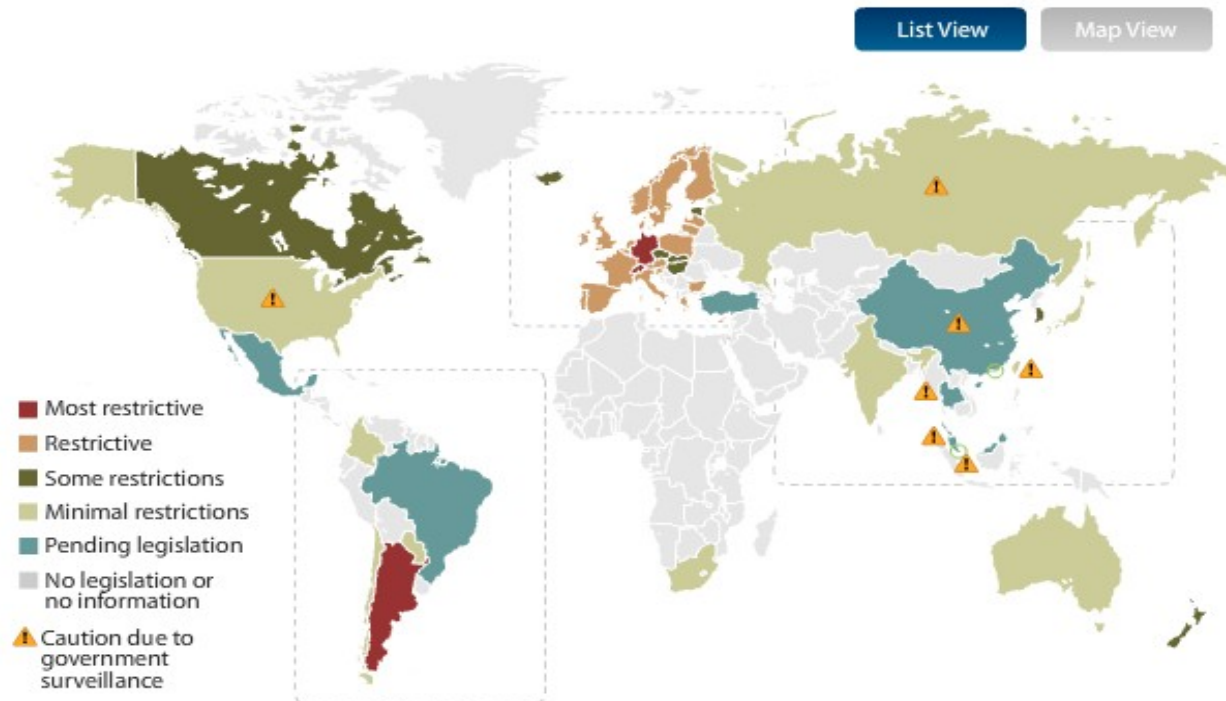
Solving the Problem

A Theoretical Approach

- **Fact:** Practical approaches on the forensic problem do obviously not work.
- **Theoretical approach:** Uncloak the black box the CSP makes out of Cloud Computing environments by using a theoretical estimation approach.
- Use modified Distributed Sensor Network (DSN) for gathering needed information and establish a Data Fusion Framework for enriching the collected data.
- **Main goal:** Forensic identification and validation of computational structures in distributed environments – at least, the investigator knows *where* to begin the investigation

Do You Know Where Your Data is in the Cloud?

Interactive Data Protection Heat Map



Source: US Department of Commerce and country specific legislation

Source: Forrester Research, Inc.

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



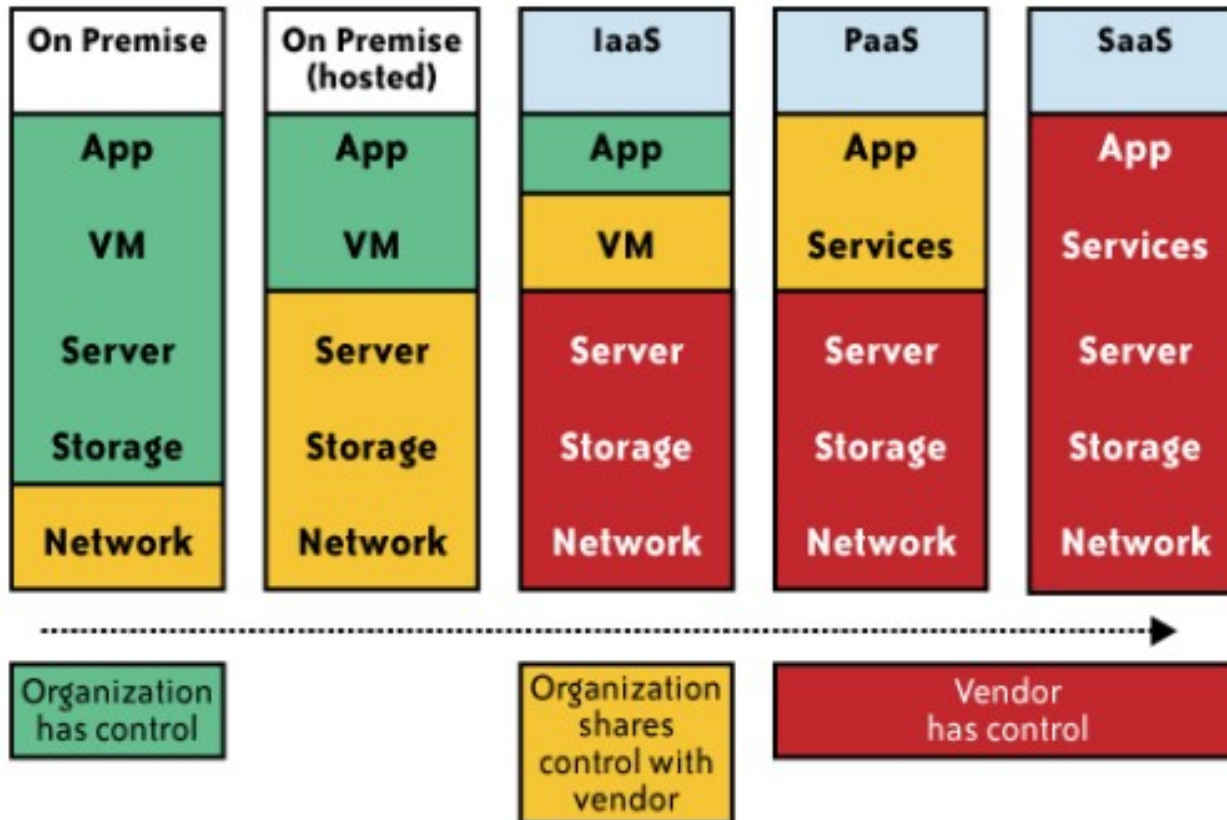
Further Unsolved Forensic Aspects

Do current SLAs help in the Context of Digital Investigations?

- Is there any knowledge about what the CSP logs and how long he keeps this information? Does the CSP vouch for the integrity of the evidential data?
- If SLAs exist, they are mostly useless in the context of digital investigations.
- Secure File Deletion: Used to not be an issue until the advent of Cloud Computing, however, who guarantees the customer that the sensitive data stored on a virtual machine has been deleted exhaustively?



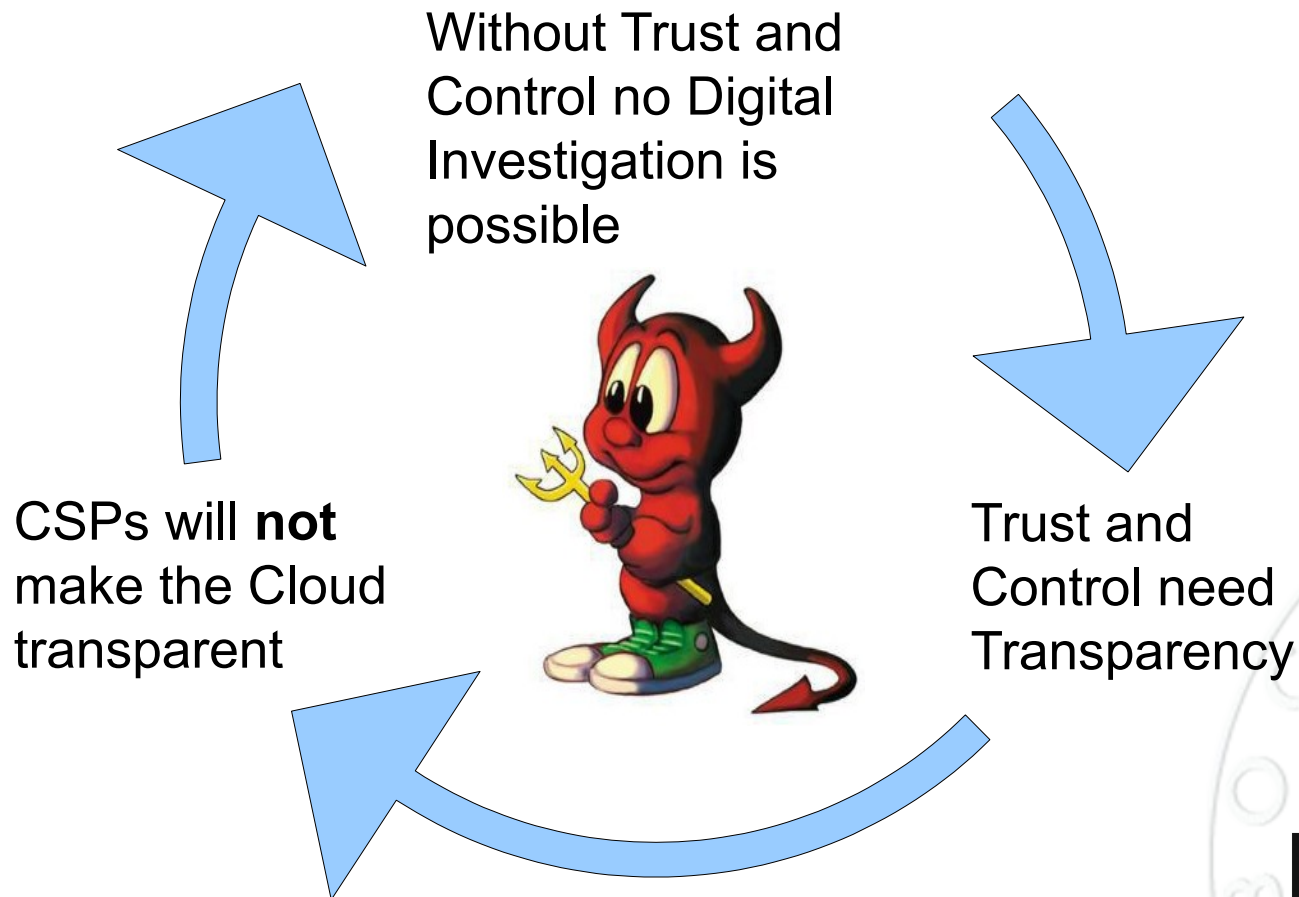
Control and Governance in the Cloud



Source: "Cloud Security and Privacy" - Tim Mather, Subra Kumaraswamy, Shahed Latif



Future Problem of Cloud Forensics



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

Threats in “Swamp Computing” Environments

- Contractual, legal and jurisdictional threats as well as threats to infrastructure assembly
- **Buzzword Bingo:**
Side channel attacks, denial of resources, resource theft, cost-overrun attacks, underprovisioning ...
- *Underprovisioning:* Imagine a CSP that discovers too late that it is hosting the Internet's next Google or Facebook → Fail of Scalability?
- *Cost-Overrun Attack:* Who pays for the implications of a Denial of Service Attack (DoS)?

For more buzzwords see: “*Self Hosting vs. Cloud Hosting: Accounting for the security impact of hosting in the Cloud*” - David Molnar and Stuart Schechter

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.



Some References

- *“On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing”* - Marten van Dijk and Ari Juels
- *“Cloud Security and Privacy”* - Tim Mather, Subra Kumaraswamy, Shahed Latif
- *“Security Guidance for Critical Areas of Focus in Cloud Computing”* - Cloud Security Alliance (CSA)
- *“Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds”* - Ristenpart et al
- *“Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments”* - Diane Barrett and Greg Kipper

Thanks for Your Attention!



Dominik Birk
dominik.birk@rub.de



Christoph Wegener
christoph.wegener@rub.de

