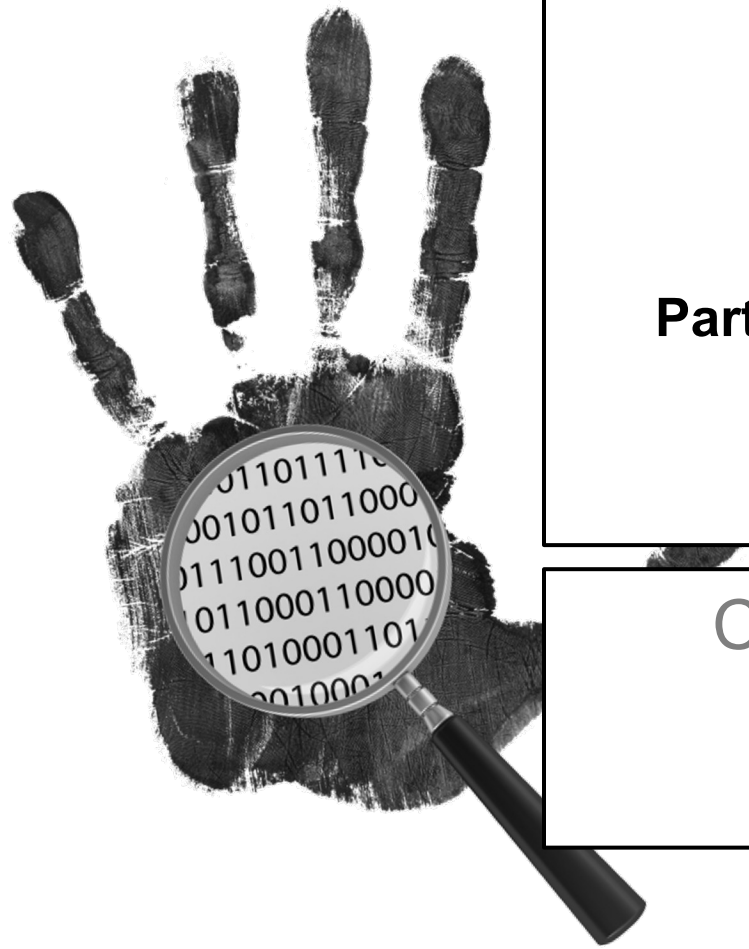
TÉCNICO LISBOA



Cloud Forensics

Part III. Specialized Techniques and Tools for Digital Forensics

CSF: Forensics Cyber-Security

Fall 2023

Nuno Santos

Previously: Mobile forensics

- Introduction to mobile forensics
  - Evidence from Android devices
  - Evidence extraction from Android devices
  - Reverse engineering of Android apps
  - Forensic analysis of Android apps

Class roadmap

- Introduction to cloud computing forensics
- Course wrap-up

TÉCNICO LISBOA

Overview of cloud computing

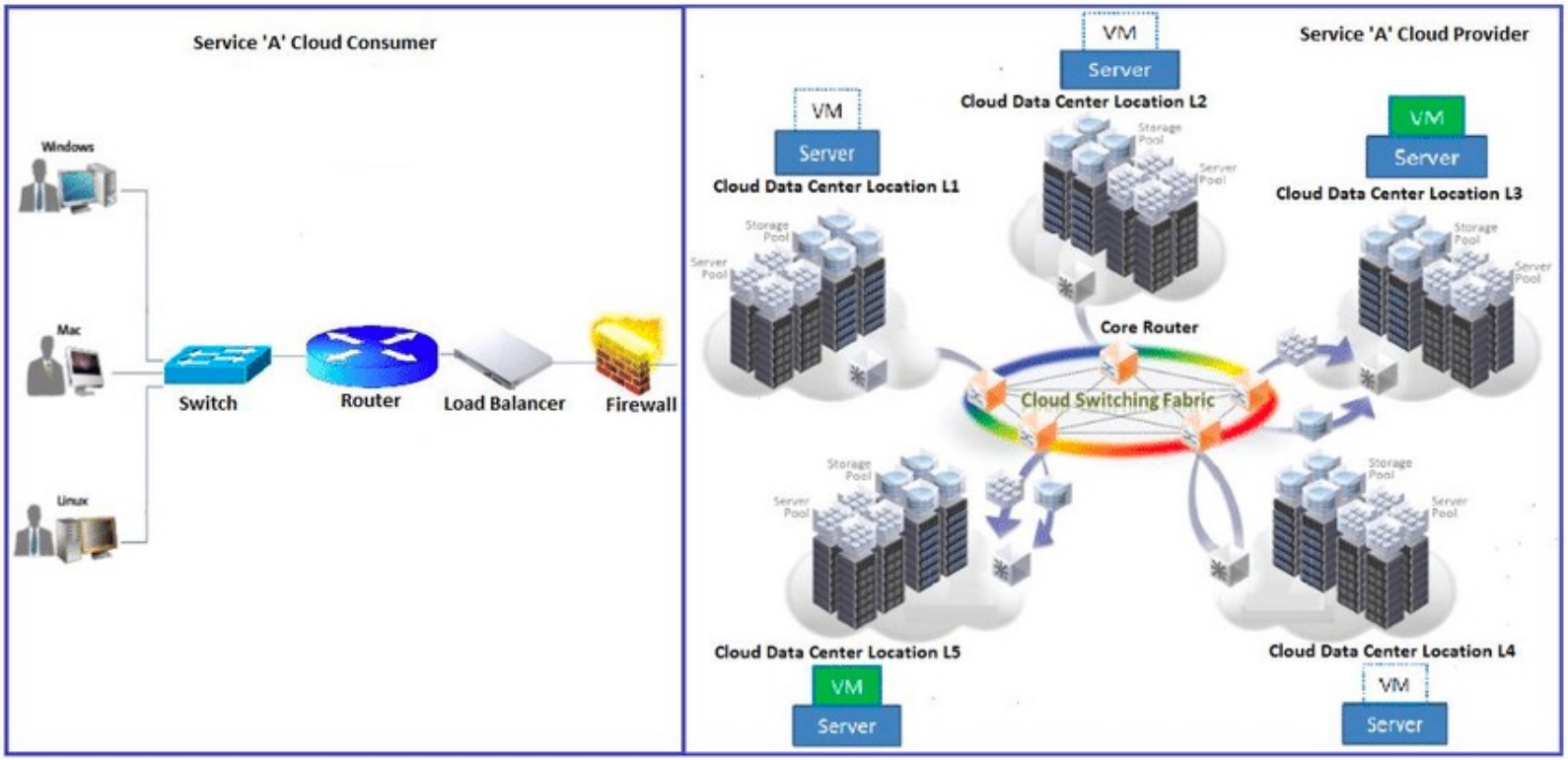
Introduction to cloud forensics

- What do we intend by cloud computing?
- What are the specific forensic challenges in cloud forensics?
- What are the main techniques for cloud forensics?

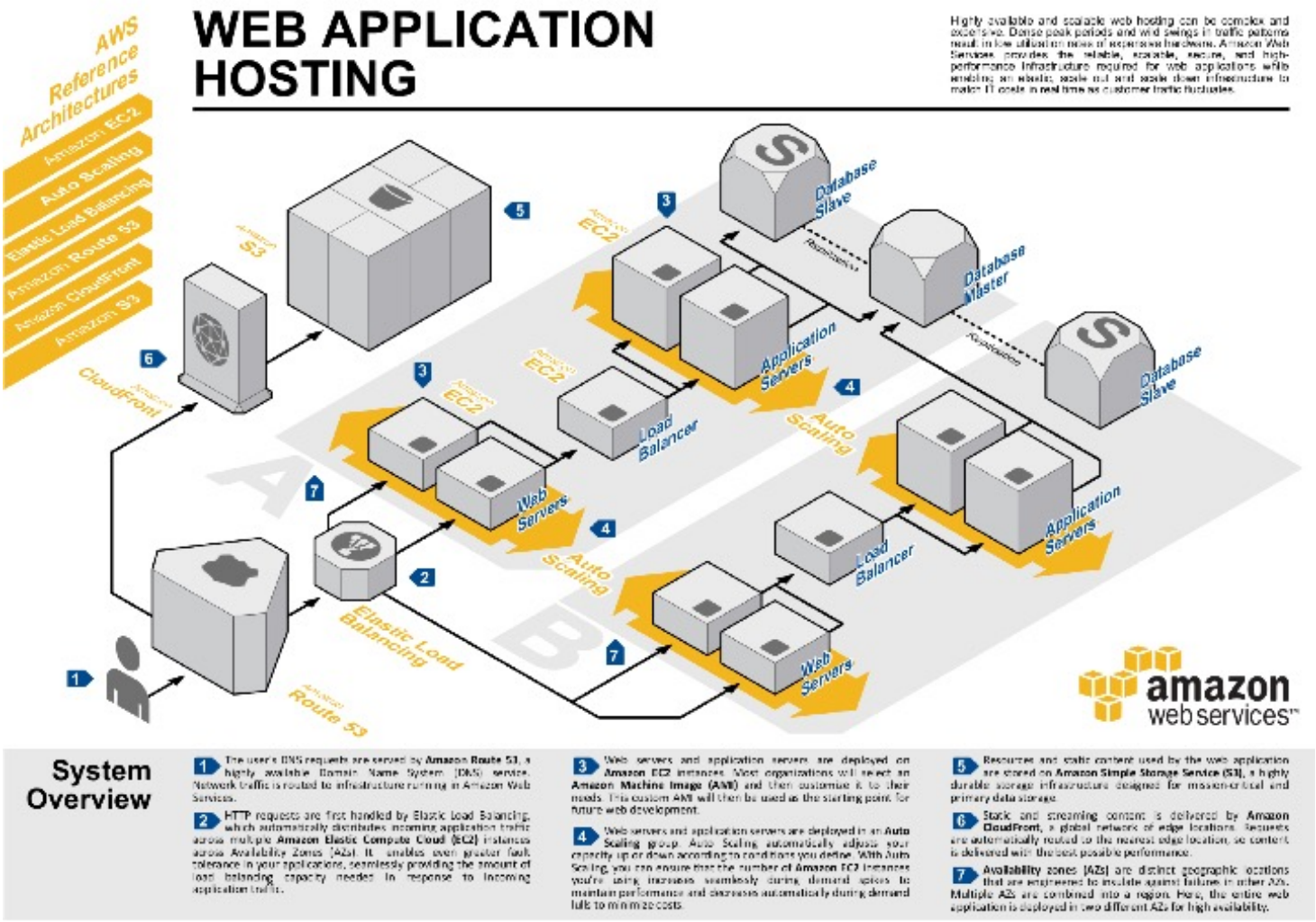
The cloud as defined by NIST

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

High level view of cloud architecture

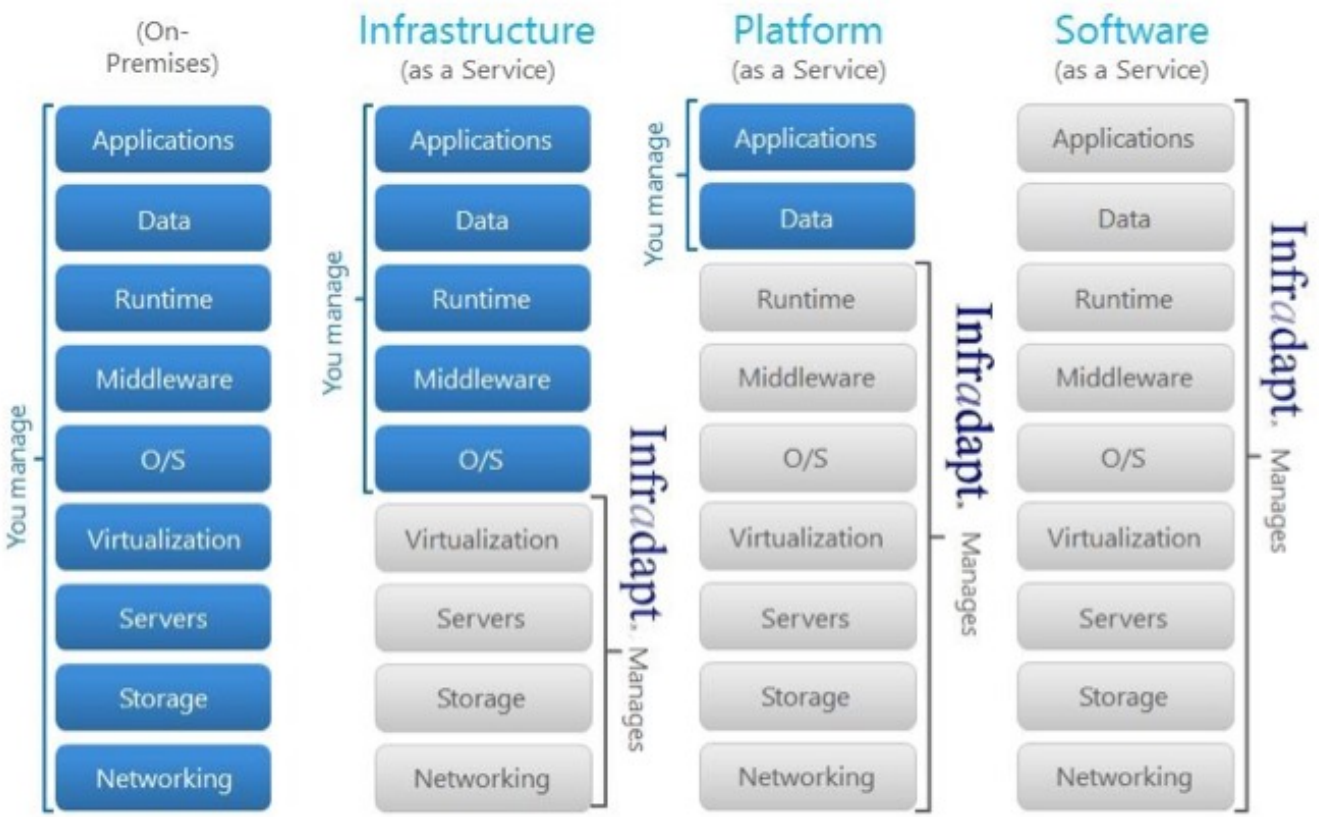


The cloud backbone: Datacenters



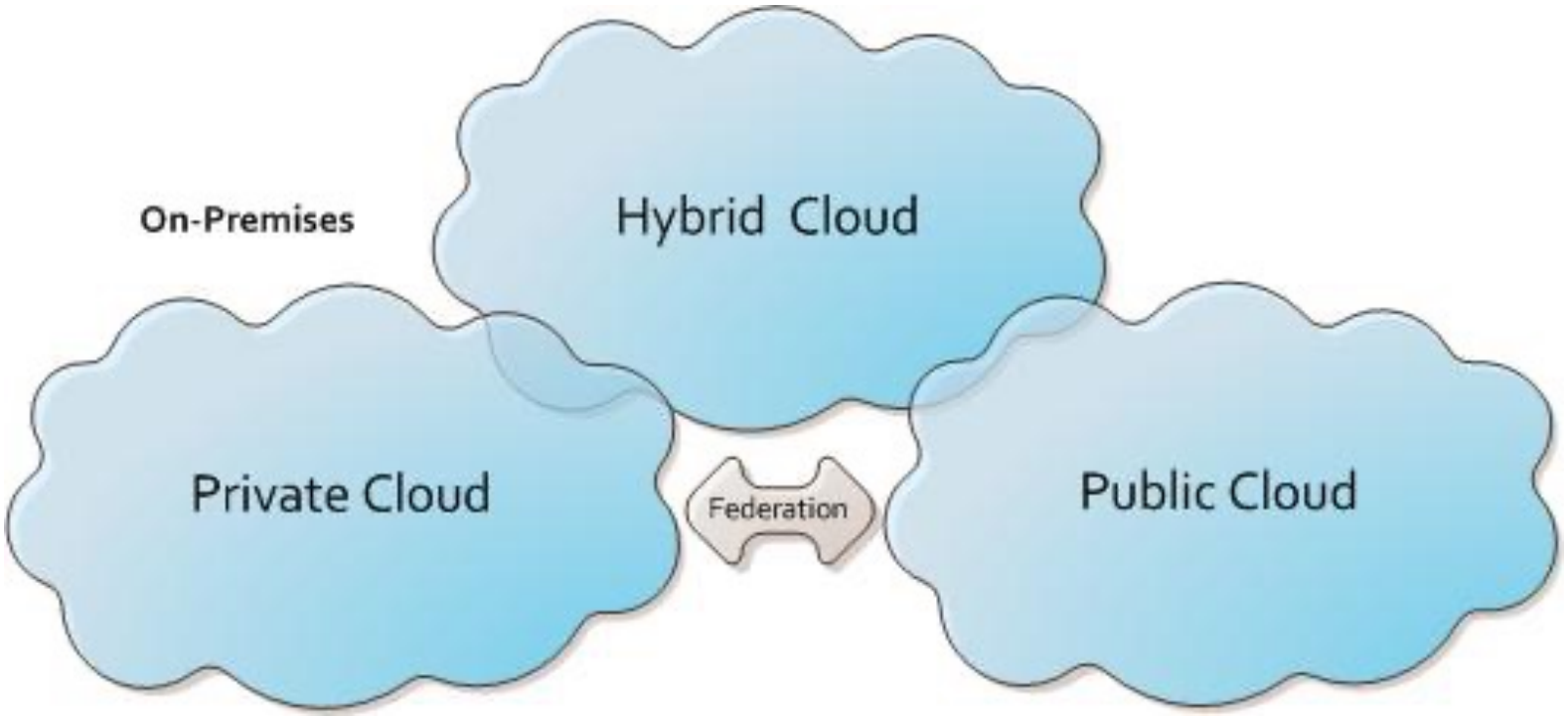
Cloud service models

- Three main models: IaaS, PaaS, and SaaS
  - Below: You – the cloud customer; Infradapt – the cloud service provider



Cloud deployment models

- Private, public, hybrid



First cloud crime

Amazon's EC2 Cloud Service Fueled PlayStation Network Attack

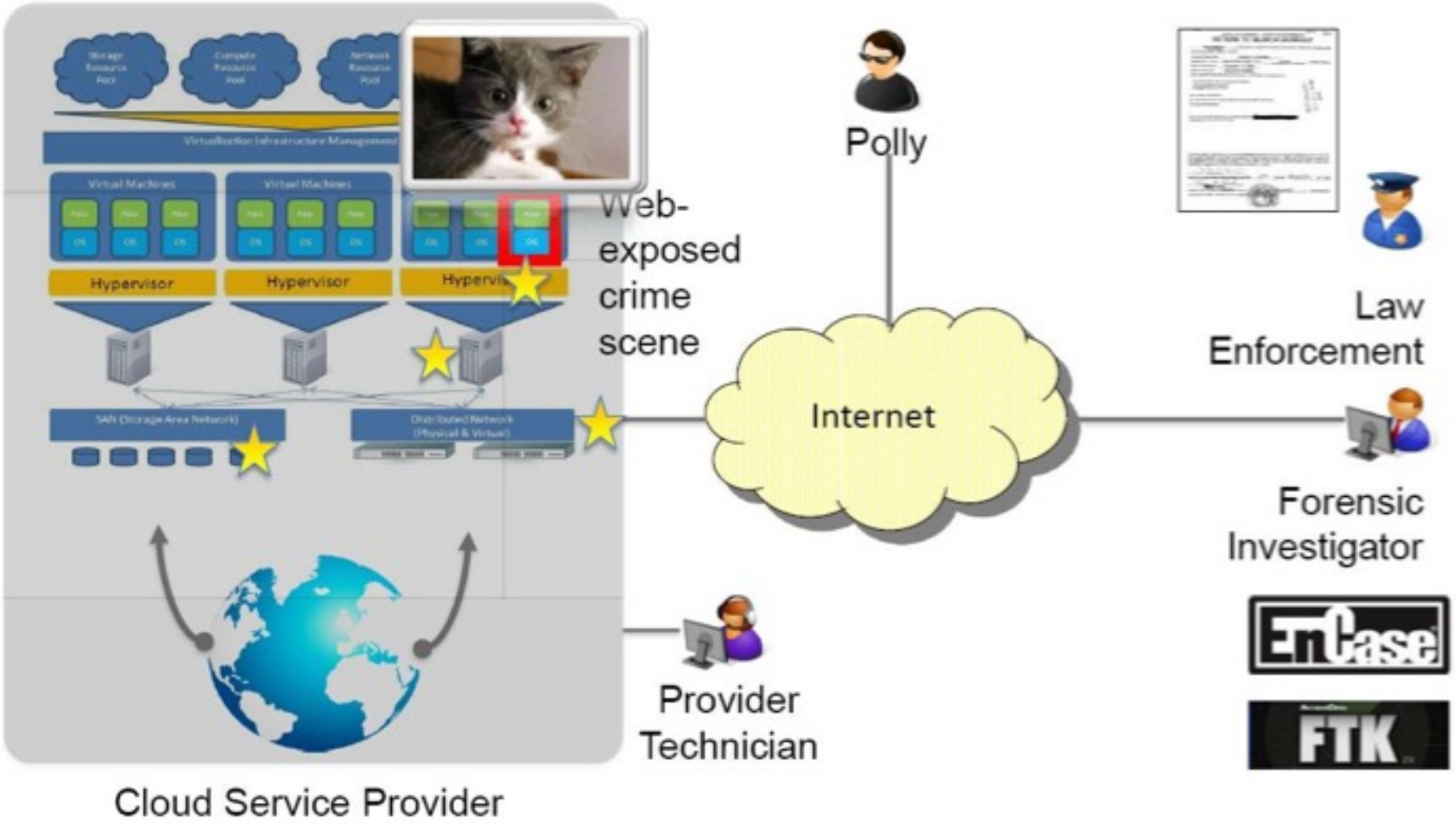
By David Murphy | May 14, 2011 03:23pm EST | 7 Comments | Email | Print

+1 0 | Share 123 | Tweet | Share 16 | 1 Digg

If you're looking for the source of the network attacks that brought down Sony's PlayStation Network—yes, it's still down—look no further than Amazon. The online retail giant didn't bring down the PlayStation Network per se, but an undisclosed source speaking to Bloomberg News has indicated that hackers used Amazon's cloud services to fuel the break-in.

According to the source, the hackers posed as a normal business and signed up for a legitimate server rental through Amazon's EC2 service—otherwise known as Amazon Elastic Compute Cloud. It's unclear how the hackers specifically used EC2 to push the attack out, which is almost as unknown a figure as the exact treasure trove of data the attackers were able to access within Sony's network.

Cloud crime scene



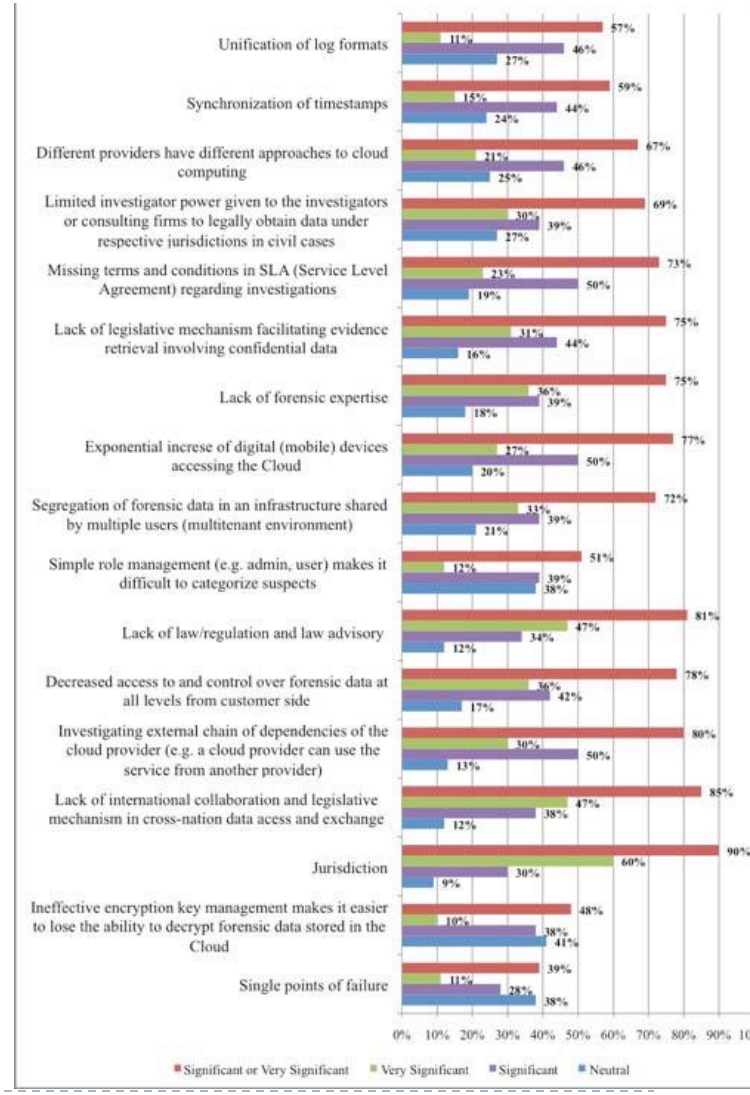
Cloud forensics as defined by NIST

"Cloud forensics is the application of digital forensics science in cloud computing environments. Technically, it consists of a hybrid forensic approach (e.g., remote, virtual, network, live, large-scale, thin-client, thick-client) towards the generation of digital evidence. Organizationally, it involves interactions among cloud actors (i.e., cloud provider, cloud consumer, cloud broker, cloud carrier, cloud auditor) for the purpose of facilitating both internal and external investigations. Legally it often implies multi-jurisdictional and multi-tenant situations. "



Some challenges

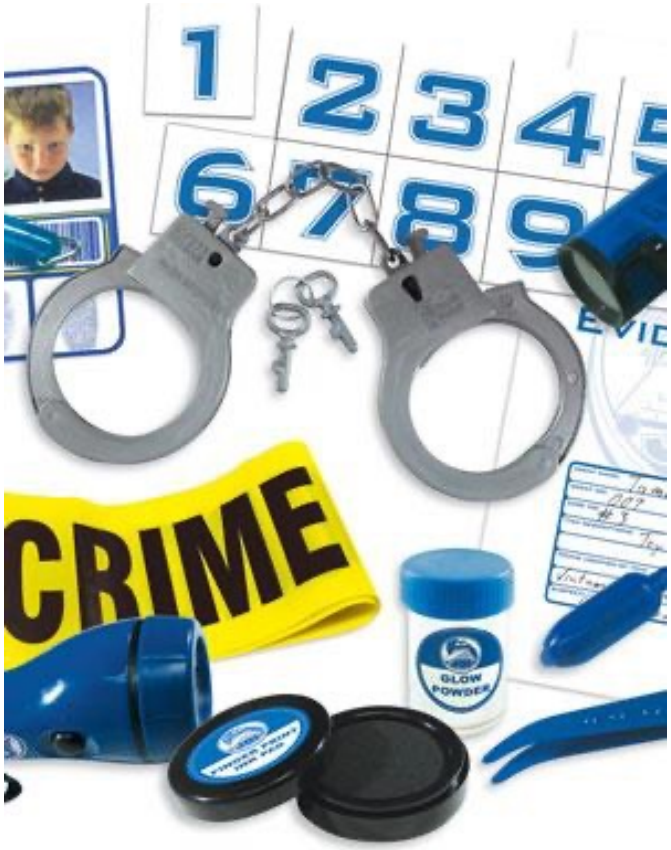
- Storage system is no longer local
- Each cloud server contains files from multiple users
- Even if data belonged to a particular subject is identified, separating it from different users is difficult
- Other than cloud service providers (CSPs), there is usually no evidence that links a given data file to a particular suspect
- Healthcare, business or national related data!



Example: Case study of child pornography

- To investigate this case, the forensics examiner needs a bit-for-bit duplication of the data to prove the existence of contraband images and video

- But in a cloud, the forensic investicator cannot collect data by himself



Obtaining a search warrant

- There are some problems with the search warrant in respect of cloud environment, for example:
  - Warrant must specify a location, but in cloud the data may not be located at a precise location or a particular storage server
  - The data can not be seized by confiscating the storage server in a cloud, as the same disk can contain data from many unrelated users
  - To identify the criminal, we need to know whether the virtual machine has a static IP
- Almost in all aspects, it depends on the transparency and cooperation of the cloud provider

Virtual Machines and volatile data

- When we turn off a Virtual Machine (VM), all the data will be lost if we do not have the image of the instance
  - If we restart or turn off a VM instance in IaaS (e.g., in Amazon EC2), we will lose all the data

- Some owner of a cloud instance can fraudulently claim that her instance was compromised by someone else and had launched a malicious activity
  - Later, it will be difficult to prove her claim as false by a forensic investigation

Trust issues

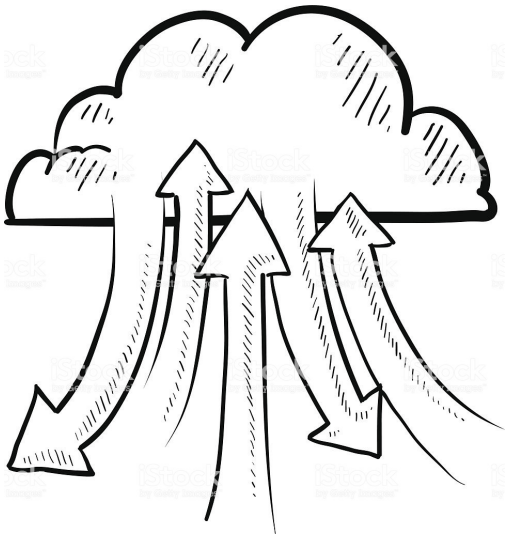
- After issuing a search warrant, the examiner needs a technician of the cloud provider to collect data
  - However, the employee of the cloud provider who collects data is most likely not a licensed forensics investigator and it is not possible to guarantee his integrity in a court of law

- The date and timestamps of the data are also questionable if it comes from multiple systems

- It is not possible to verify the integrity of the forensic disk image in Amazon's EC2 cloud because Amazon does not provide checksums of volumes, as they exist in EC2

Large bandwidth requirements

- In traditional forensic investigation, we collect the evidence from the suspect's computer hard disk
- Conversely, in cloud, we do not have physical access to the data
- One way of getting data from cloud VM is downloading the VM instance's image
- The size of this image will increase with the increase of data in the VM instance
- We will require adequate bandwidth and incur expense to download this large image



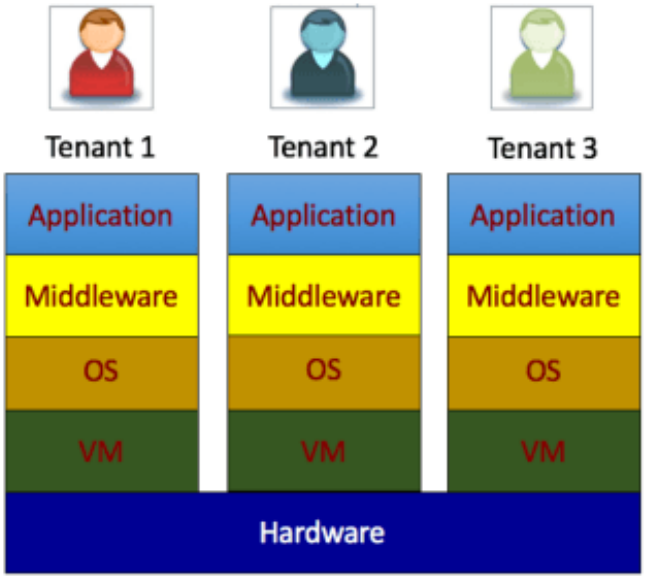
Amazon S3

Q: Where is my data stored?

Amazon S3 offers storage in the US Standard, US West (Oregon), US West (Northern California), EU (Ireland), Asia Pacific (Singapore), Asia Pacific (Tokyo), South America (Sao Paulo), and AWS GovCloud (US) Regions. You specify a Region when you create your Amazon S3 bucket. Within that Region, your objects are redundantly stored on multiple devices across multiple facilities.

Multi-tenancy issues

- Multiple VM can share the same physical infrastructure, i.e., data for multiple customers may be co-located
  - This nature of clouds is different from the traditional single owner computer system
- How to prove that data were not comingled with other users' data?
- How to preserve the privacy of other tenants while performing an investigation?
- How to ensure that VM isolation has not been violated through side-channel attacks?



Logging

- Process logs, network logs, and application logs are really useful to identify a malicious user

- Not as simple as it is in privately owned computer system:
  - Decentralization
  - Volatility of logs
  - Multiple tiers and layers
  - Accessibility of logs
  - Dependence on the CSP

Conducting a cloud investigation

- The type of incident determines how to proceed with planning the investigation

- If the investigation involves searching for and recovering data from cloud storage or cloud customers

Investigating CSPs

- If a CSP has no team or limited staff, investigators should ask questions to understand how the CSP is set up:
  - Does the investigator have the authority to use cloud staff and resources to conduct an investigation?
  - Is there detailed knowledge of the cloud's topology, policies, data storage methods, and devices available?
  - Are there any restrictions on collecting digital evidence from remote cloud storage?
  - For e-discovery demands on multitenant cloud systems, is the data to collect commingled with other cloud customers' unrelated data? Is there a way to separate the data to prevent violating privacy rights or confidentiality agreements?
  - Is the data of interest to the investigation local or remote? If it's in a remote location, can the CSP provide a forensically sound connection to it?

Investigating cloud customers

- If a cloud customer doesn't have the CSP's application installed
  - You might find cloud-related evidence in a Web browser's cache file
- If the CSP's application is installed
  - You can find evidence of file transfers in the application's folder
  - Usually found under the user's account folder

Tools for cloud forensics

- Few tools designed for cloud forensics are available
- Many digital, network, and e-discovery tools can be combined to collect and analyze cloud data
- Some vendor with integrated tools:
  - Guidance Software EnCase eDiscovery
  - AccessData Digital Forensics Incident Response
  - ProDiscover Incident Response and Forensics

Limitations of current forensic tools

- Due to the distributed and elastic characteristic of cloud computing, the available forensic tools cannot cope up with this environment
- **Tools and procedures are yet to be developed for investigations in virtualized environment, especially on hypervisor level**
- Need of forensic tools for the CSP and the clients to collect forensic data

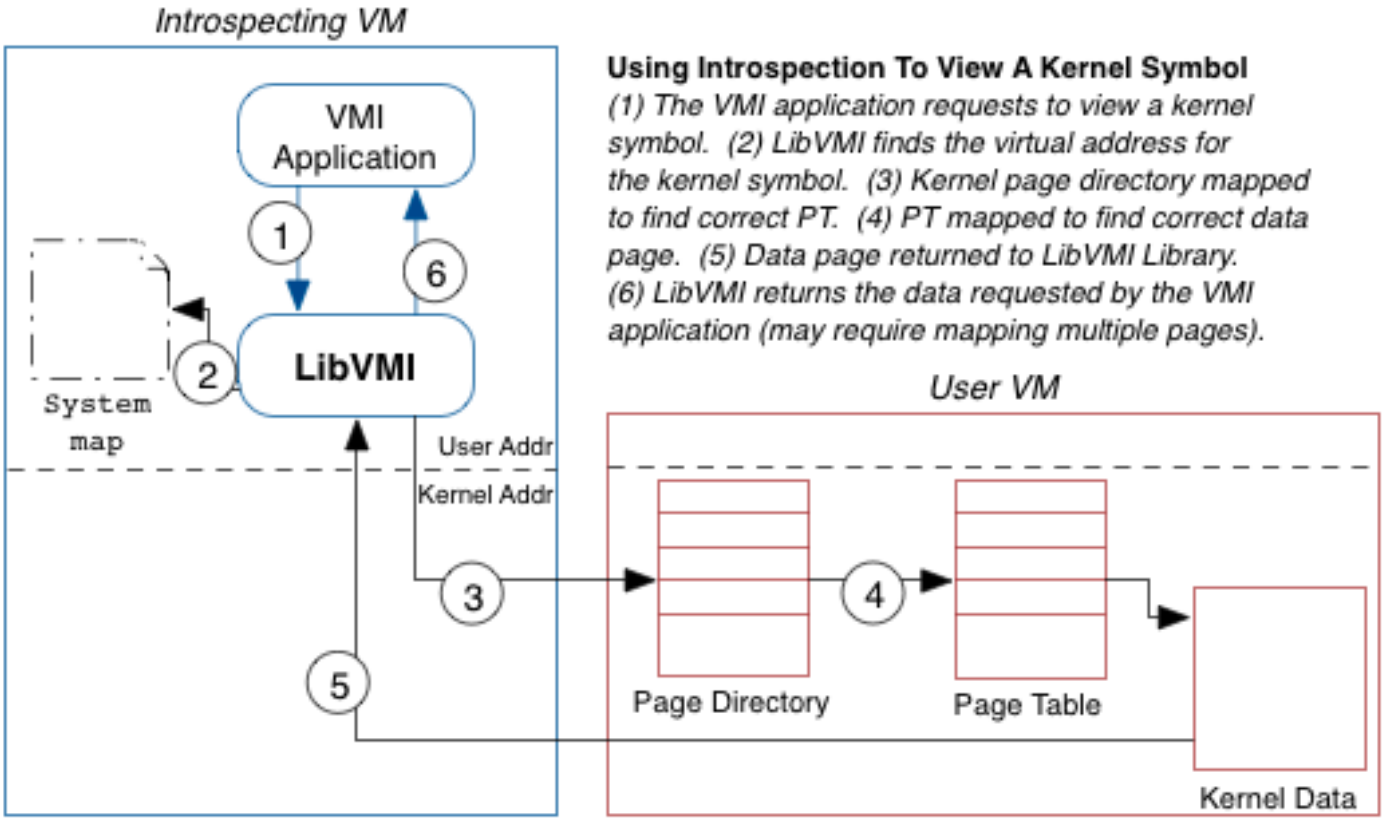
Virtual Machine Introspection

- Virtual Machine Introspection (VMI) is the process of externally monitoring the runtime state of VM from either the Virtual Machine Monitor (VMM), or from some virtual machine other than the one being examined

- By runtime state, we are referring to processor registers, memory, disk, network, and other hardware-level events

- Through this process, we can execute a live forensic analysis of the system, while keeping the target system unchanged

How does VMI work



- http://libvmi.com/docs/gcode-intro.html

TÉCNICO LISBOA

Course wrap-up

Course program review

- Part I: Foundations of digital forensics
  - Legal framework, digital investigation, evidence acquisition…
- Part II: General techniques and tools for digital forensics
  - Files, steganography, storage, file systems, OSes, packet analysis, email, web…
- Part III: Specialized techniques & tools for digital forensics
  - Rootkits, anonymization, botnets, cryptocurrency, cloud forensics…

Upcoming

- Project discussions
  - The calendar of the discussions has been published
  - Changes to slot allocations must be done until the end of this week

- Exams
  - November 10th, 15h30
  - Recovery exam: January 31st, 13h00
  - Don't forget to enroll in the exams!

Good luck for the discussions and exams!

Exercises

- 2020/21 – 2nd Exam: III.1.h
- 2019/20 – 1st Exam: III.1.h