Hasso Plattner Institut

IT Systems Engineering | Universität Potsdam

Cloud Computing Security

Master Seminar, Summer 2011

Maxim Schnjakin, Wesam Dawoud,
Christian Willems, Ibrahim Takouna
Chair for Internet Technologies
and Systems

„Definition“ of Cloud Computing

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

Benefits

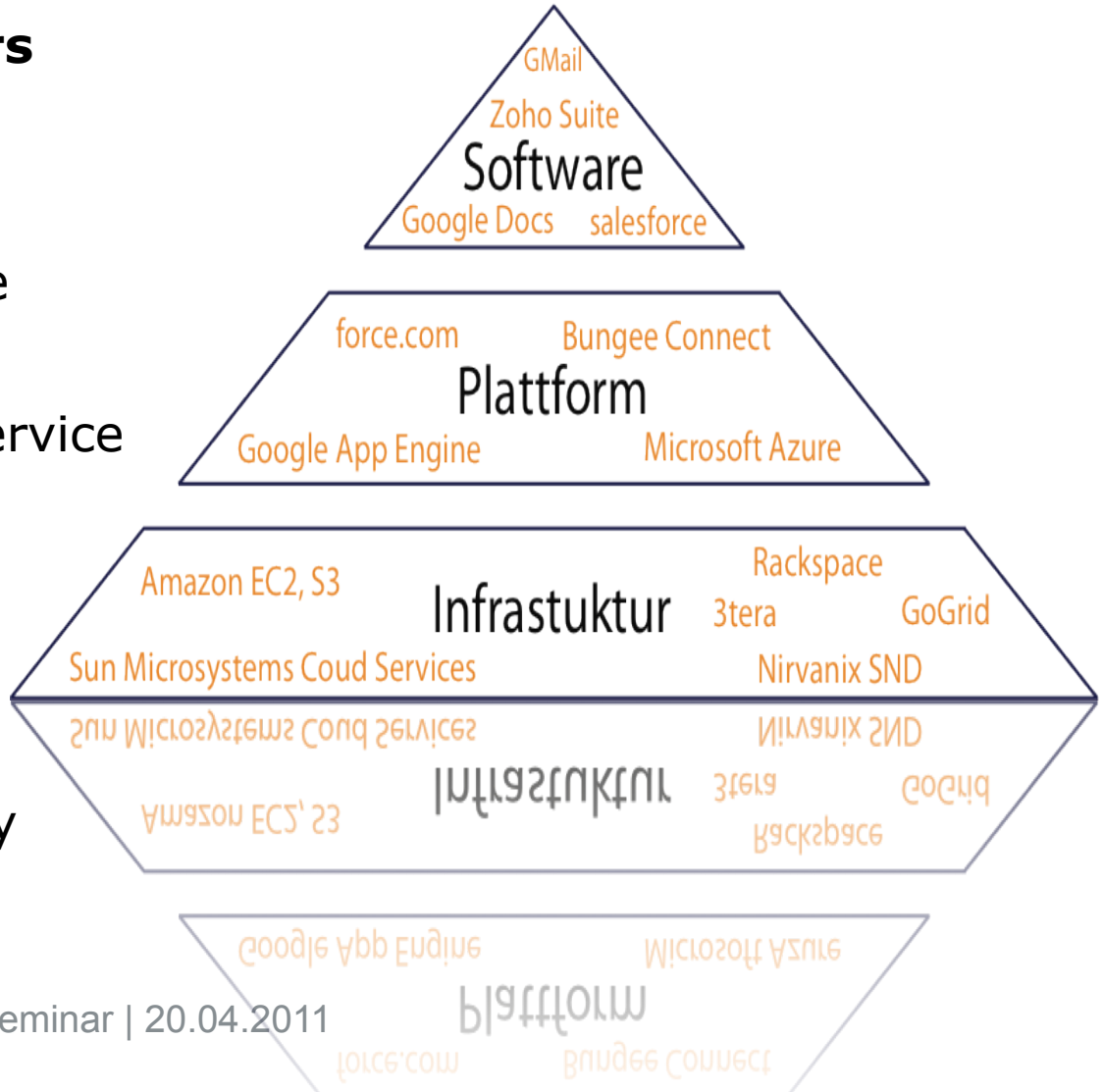
- Flexibility
  - Rapid provisioning of services
- Mobility
  - High availability of services
- Reduced Cost
  - Economies of economies of scale
  - Low-cost disaster recovery and data storage solutions ...
  - The elimination of up-front commitment
  - The ability to pay for use of computing resources
- ...

Architecture

Different Service Layers

- Software as a Service (SaaS)
- Plattform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

- Below: Hypervisor technology



Challenges

- Reliability and availability
  - Failures do occur
- Privacy & Security
  - Loss of physical control
  - Trusting vendor‘s security model
  - Vendor or data lock-in is possible

Challenges

- Missing Service Level Agreement (SLA) Standardisation
  - In the future an abundance of cloud services and providers is expected
  - The selection of a proper provider becomes more difficult
  - The problem of service level management in inter-domain scenarios is not solved up to today

Mode of operation

Working on topics ...

- ... in groups of 2-3 students
- ... in close consultation with the tutors
- ... presenting results 2-3 times during the semester
- ... finishing with a final report at the end of the semester

„Leistungserfassung“

- 6 ECTS, with mark
- Presentations
- Paper (12-15 pages)
- Active discussion in the seminar
- Paper deadline: 23.07.2011

Topic: Hypervisor Security

Different categories for attacks on hypervisors:

- against **hypervisor** itself
  - Break out of virtual machines
  - Attacks via communication channels
  - Denial-of-Service
  - ...
- against **other virtual machines**
  - Tampering, resource limitation / Denial-of-Service
  - Hijacking other virtual machines (Guest Hopping)
  - Eavesdropping
  - ...

Examples:

- **Red Pill / Blue Pill**
  - Blue Pill is a hypervisor-based rootkit system
    → injection of a thin hypervisor at runtime
  - Hackers from Invisible Things Lab managed to inject Blue Pill below a Xen hypervisor!
- Overload situation by causing **I/O blockade**
  - CPU can safely be distributed among guest machines
  - More difficult with I/O access
  - How and under which circumstances can a malicious VM slow down other VMs by causing loads of I/O operations?

Topic: Hypervisor Security

Topic distribution

- Several groups possible:
  → investigation on different hypervisors and aspects
  - VMware
  - Xen
  - ...

General Topic

- Research and classification on attacks and exploits
- Testing of existing exploits against different hypervisors

Project 1

- Exerimenting with hypervisor overloading
- Creating a framework for measuring overload

Topic: Hypervisor Security

Project 2: Possible attacks on Xen 3.x Hypervisor

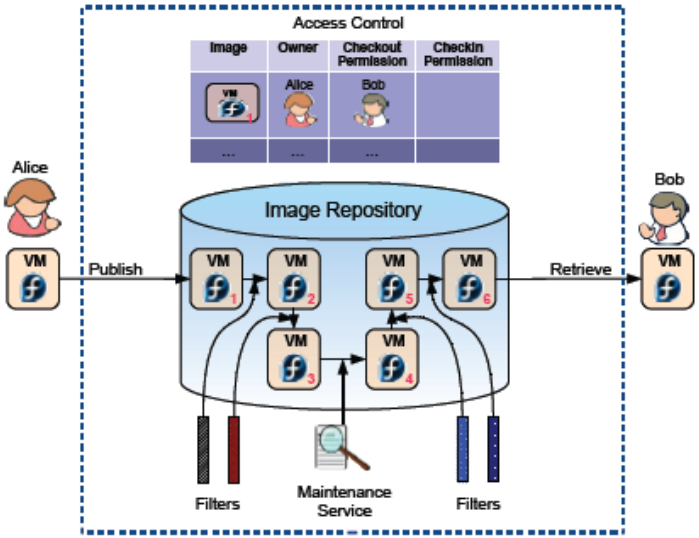
- Hypervisor attacks via DMA
- Generic attack using disk controller
- Hypervisor backdooring
  - "DR" backdoor
  - "Foreign" backdoor
- Applying the same attacks on Xen 4.x Hypervisor

Project 3: Assessing and Hardening the virtual networking infrastructure

- Investigate networking modes in each hypervisor.
- Compare the security of networking in different virtualized environments (e.g. Xen-based environment vs. VMware-based environment)

Virtual Machines repository security

- The problem:
  - Anybody can upload VM image into Amazon repository.
  - These machines can contain worms, viruses, or backdoors which can't be easily discovered by the user.
  - Infected images can be offered to the public users to use.
  - The number of these machines increase with the time.
  - These machine could be an infrastructure for Distributed DoS attack.



Topic:
Infrastructure as a Service Security

Project 4: Classifying VMs images and tracking the relations

- Build the necessary experimental setup (e.g. install Xen, Eucalyptus, S3, etc…)
- Classify the VMs images in the repository according to: OS, Architecture, Distribution, Kernel version, etc…
- Keep track of the VMs relations (e.g. Parent-Child), this relations will ease and reduce scanning and maintenance time.

Project 5: Online and offline filtering for the VMs image

- Build the necessary experimental setup (e.g. install Xen, Eucalyptus, S3, etc…)
- Develop filters remove VM publisher sensitive data (e.g. Browsers history, cookies, shell history, etc...)
- Develop filters detect malicious images and remove malicious contents.

Topic: SLA in the Cloud

Status quo:

- **No** standards
  - SLA are often written in natural language
- Vendors differ in pricing scheme
  - amount of data stored
  - bandwidth consumed in transfers
  - HTTP and REST requests

Aim of the project:

- Definition of uniform storage service description
- Identification of service providers based on users expectations

Project Context