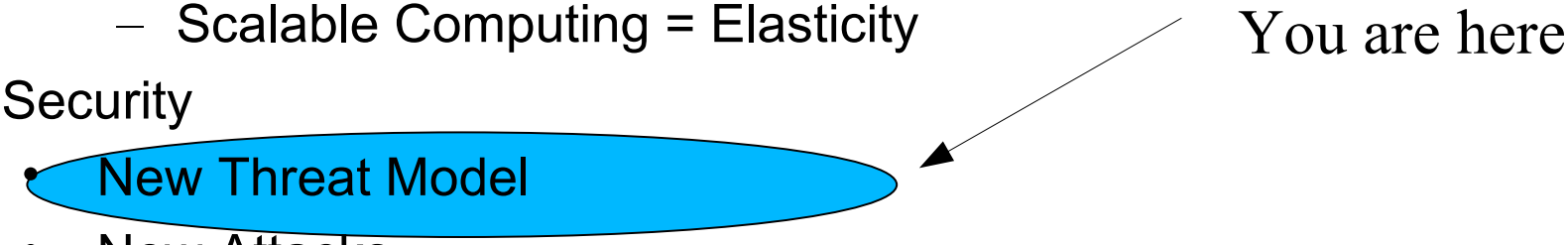
Threat Model for Cloud

Fabrizio Baiardi
f.baiardi@unipi.it

Cloud Syllabus

- Supporting Technologies
  - Virtualization Technology
- Cloud Computing Introduction
  - Definitions
  - Economic Reasons
  - Service Model
  - Deployment Model
  - Scalable Computing = Elasticity
- Security
  - New Threat Model
  - New Attacks
  - Countermeasures



Before the threats, the problem to be solved

- When moving your application and data to the cloud, you no longer have to protect resources (processor, memory, networks)
- Instead you have to protect your information
- Information-centric security binds security directly to information and the people who access it to ensure that they can access only the right information at the right time, when and where they need it
- All the assets you have to protect are virtual
- The cloud provider, instead, has always to protect the physical assets
- No perimeter to be defended

Threat models and cloud migration: before

- They (evil, the external threat)
- Us (good ones)
- Us (the bad ones, insider threat)
- The defence is based upon
  - Preventing an attacker from entering into/interacting with the system (firewall)
  - Discovering insider behaviours that violate the security policy or that have defeated the firewall (host & network IDS)
- The approach can be more complex (e.g. defence in depth) but the distinction based upon a number of perimeters is always there
- Zero trust network is one of the few cases where the perimeter is not important because trust depends on the user and the underlying device

Threat models and cloud migration: after

- They (evil, the external threat)
- Us (good ones but also the bad ones and insider threats)
- We share the physical infrastructure, our application, our data with the evil, the cloud provider can be evil
- Now every threat becomes also an insider threat
- The virtualization support, the VMMs, has
  - to implement VMs
  - share physical resources among them
  - confine anomalous and dangerous users from good ones
- The attack surface of the cloud system, the target system, increases at it includes
  - The VMM
  - The browser that is used to interact with the cloud.

Extended Attack Surface

- The attack surface of a system includes all the modules that may be the target of an initial attack in an intrusion that enables the threat to reach some goals
  - Entry points
  - Exit points
  - Channels
- The notion of surface allows us to evaluate the percentage of a system exposed to threat attacks = how many initial attacks with respect to all possible attacks
- The attack surface of a cloud system is larger than the one of an equivalent stand alone system

How much control on the assets and the VMM?

- Private cloud
  - used by a single organization eg a university, a company
  - good control
- Community cloud
  - used by a set of organizations that should share the same security policy eg several hospitals
  - acceptable control
- Public cloud
  - No control

New classes of attacks

A system where legal user and attacker share the same architecture is the target of new attacks that

- discover and monitor the flows of information
  - among VMs, application, platforms
  - between the browser and the cloud
- discover the allocation of VMs onto physical nodes to deduce the physical resources shared among VMs =

  cloud cartography
- control the user browser to control and manipulate the cloud resources with respect to attacks that steal info of a browser

  = when considering clouds the attacker goal is to control those resources accessed through the browser

However, there is a much larger amount of cheap processing power, Can this power be helpful for the good guys? How?

SaaS Maturity Levels

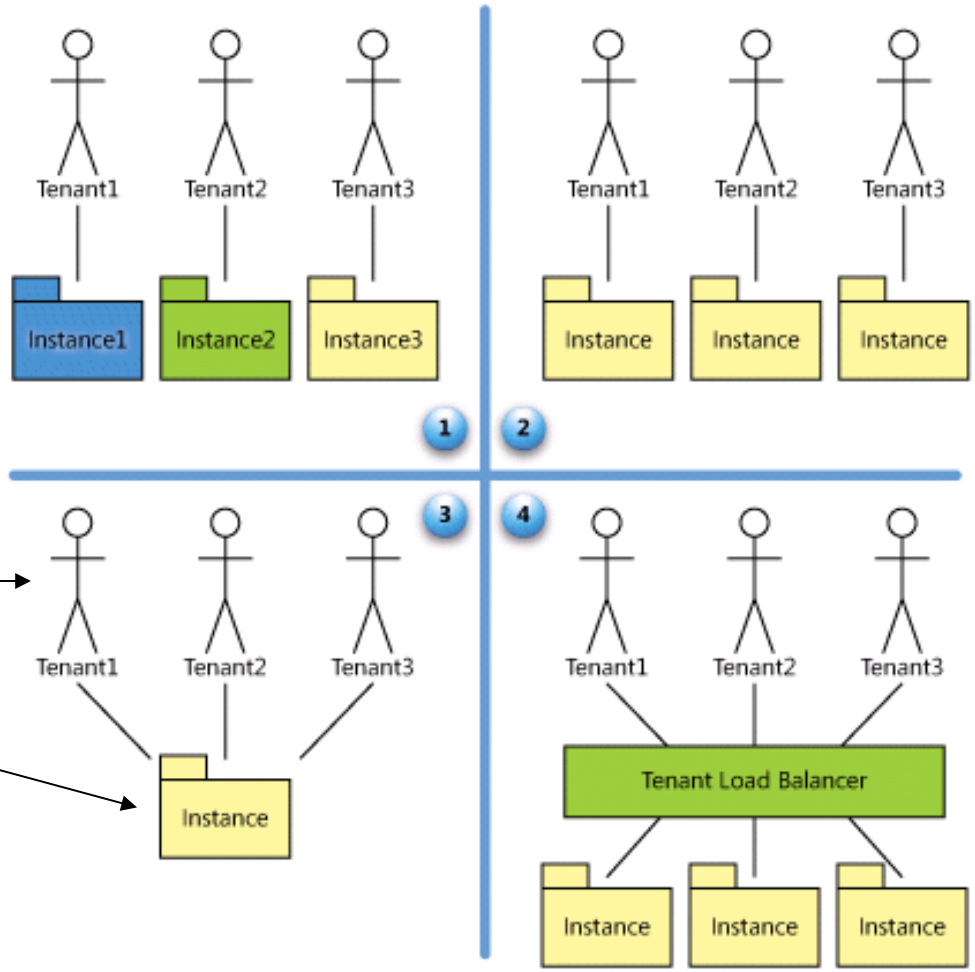
Level 1: Ad-Hoc/Custom

Level 2: Configurable

Level 3: Configurable, Multi-Tenant-Efficient

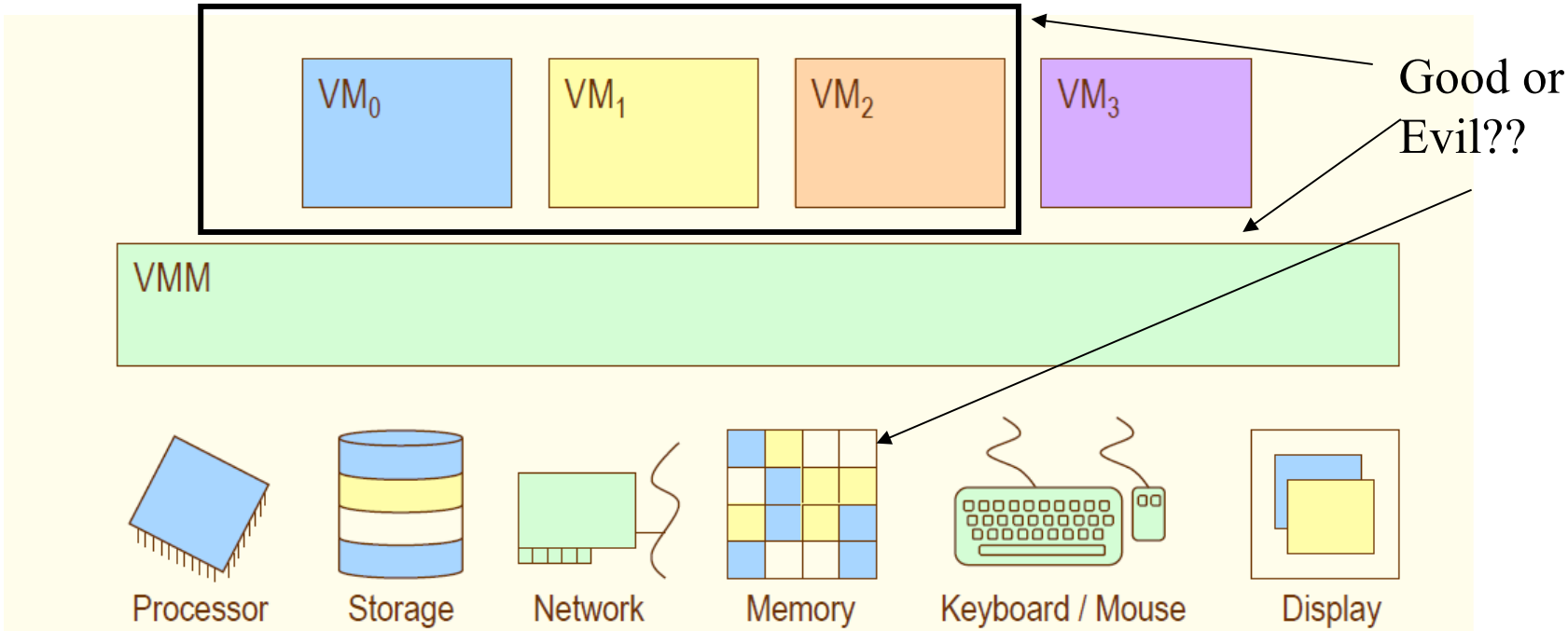
Level 4: Scalable, Configurable, Multi-Tenant-Efficient

Good or Evil?



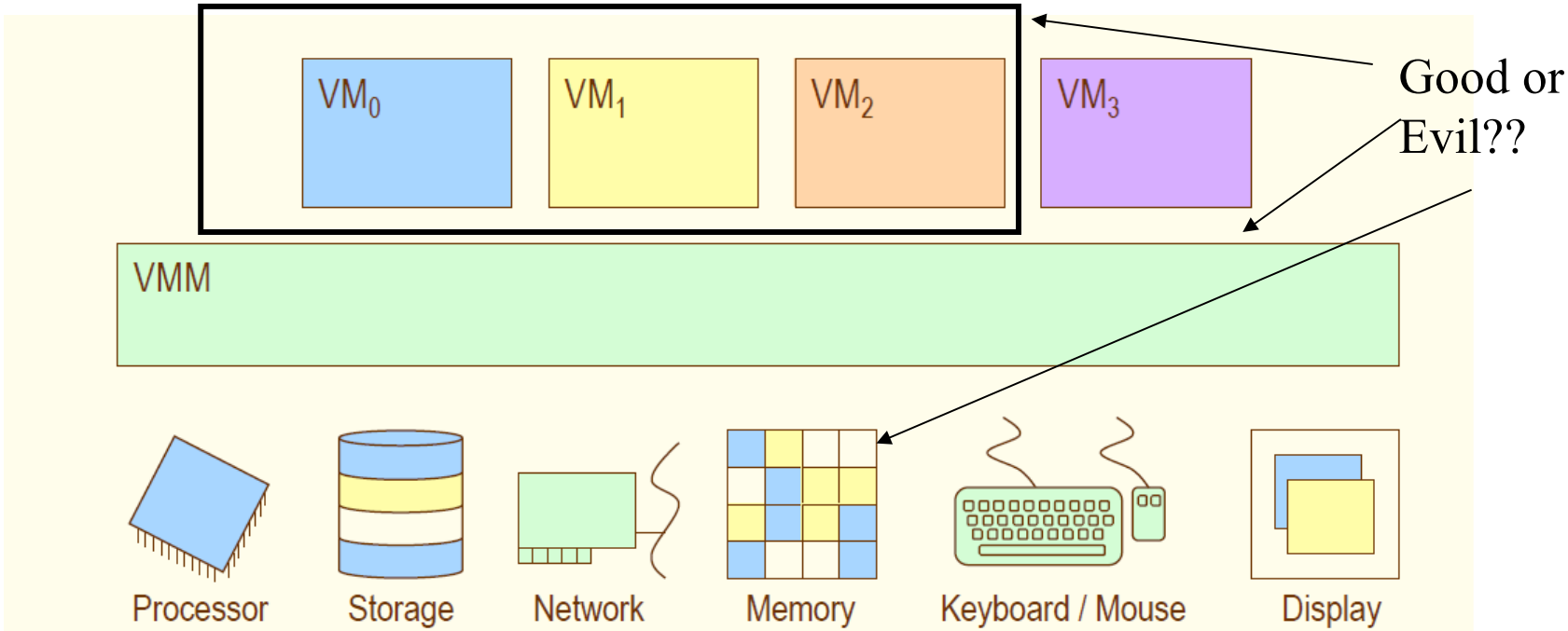
Source: Microsoft MSDN Architecture Center

All together ????



- **VMM applies all 3 sharing methods, as needed, to create illusion of platform ownership to each guest OS**

All together ????



- **VMM applies all 3 sharing methods, as needed, to create illusion of platform ownership to each guest OS**

New resource availables for attacker

- A cloud is an interesting target for several threat such as terrorist or organized crime
- After a successful attack, the attacker can access a much larger amount of resources, know how, processing power than typical attackers
- The large amount of cheap processing power that cloud systems offer simplifies the implementation of brute force attacks, e.g. exhaustive key searches
- A side effect is that a SME has to face a trade off
  - Better security offered by the provider
  - More powerful attackers

The cloud provider

- It is a new threat to be considered
- Why so few papers discuss this threat ??? :-D
- The impact of a provider attack is highly critical because of the kind of access to physical and logical resources
- Some problems are independent of malicious planned attack
  - Lock in with a provider in the case of SaaS
  - It is almost impossible to have some assurance that the provider has erased data stored in the cloud
- With respect to other threats, the provider is known, hence we simply need to prove a misbehavior rather than detailing which misbehaviour the provider has been involved in

The cloud provider

- A Service Level Agreement (contract) defines
  - The amount of resources that will be available
  - Largest downtime that is acceptable
  - Geographical location of the data
  - Handling of sensible data
  - Use of encryption
  - Security policy of the provide
- Only include properties that can be measured and hence checked = Only include what can be measured
- Automate to simplify the check implementation and increase the number of checks executed for the same cost= only include what can be automatically measured

Cloud Vulnerabilities

- What follows is a long(and tedious) list of vulnerabilities
- Some of them will be discussed in the following, other ones are to be remembered when checking a provider or writing a SLA since there are no new countermeasures
- This is a checklist, checklists are tedious but unbelievable useful when needed

Authentication Vulnerabilities

Access and Autentication

- Insecure storage of cloud access credentials by customer
- Insufficient roles available
- Credentials stored on a transitory machine
- Password-based authentication may become insufficient
  - Strong or two-factor authentication for accessing cloud resources will be necessary

Authentication Vulnerabilities

- Identity of customer or billing information is not adequately verified at registration
- Delays in synchronization between cloud system components
- Multiple, unsynchronized copies of identity data are made
- Credentials are vulnerable to interception and replay
- De-provisioned credentials are still valid due to time delays in roll-out of revocation

Resource Vulnerabilities

Inaccurate Modeling of Resource Usage

- Overbooking or over-provisioning (on demand …)
- Failure of resource allocation algorithms due to extraordinary events (e.g., outlying news events for content delivery).
- Failure of resource allocation algorithms using job or packet classification because resources are poorly classified.
- Failures in overall resource provisioning vs temporary overloads

No resource capping (quotas)

- If there is not a flexible and configurable way for the customer and/or the cloud provider to set limits on resources, this can be problematic when resource use is unpredictable.

Inadequate Resource Provisioning and Investments in Infrastructure

- Infrastructure investments take time. If predictive models fail, the cloud provider service can fail for a long period.

Vulnerabilities

Remote Access To Management Interface

- Allows vulnerabilities in end-point machines to compromise the cloud infrastructure (single customer or CP) through, for example, weak authentication of responses and requests

Hypervisor

- Exploiting the hypervisor potentially means exploiting every VM!
- Guest to host escape: A user defeat isolation and exit from a VM
- VM hopping: After leaving a VM other are attacked
- Virtual machine-based rootkits

Isolation Vulnerabilities

Lack of Resource Isolation

- Side channel attacks
- Shared storage
- Insecure APIs
- Lack of tools to enforce resource utilization

Lack of Reputation Isolation

- Activities from one customer impact the reputation of another customer and of the cloud provider

Communication Encryption

- Reading data in transit via MITM attacks
- Poor authentication
- Acceptance of self-signed certificates

Vulnerabilities

Weak or No Encryption Data in transit

- Data held in archives and databases
- Un-mounted virtual machine images = similar to traditional backups
- Forensic images and data, sensitive logs and other data at rest put customer data at risk

Unable to Process Data in Encrypted Form

Poor Encryption Key Management

- Hardware security modules (HSM) required in multiple locations
- Key management interfaces which are accessible via the public Internet
- The rapid scaling of certificate authorities issuing key pairs to new virtual machines (configuration of VM)
- Revocation of keys for decommissioned virtual machines

Vulnerabilities

Low Entropy for Random Number Generation

- The combination of standard system images, virtualization technologies and a lack of input devices means that virtual systems have much less entropy than physical RNGs

No Control of Vulnerability Assessment Process

- Restrictions on port scanning and vulnerability testing are an important vulnerability which, combined with an Acceptable Using Policies which places responsibility on the customer for securing elements of the infrastructure, is a serious security problem

Internal (Cloud) Network Probing

- Cloud customers can perform port scans and other tests on other customers within the internal network

Vulnerabilities

Co-residence Checks

- Side-channel attacks exploiting a lack of resource isolation allow attackers to determine which resources are shared by which customers

Lack of Forensic Readiness

- While the cloud has the potential to improve forensic readiness (vm freezing etc) several providers do not provide appropriate services and terms of use to enable this.

Vulnerabilities

Media Sanitization

- Shared tenancy of physical storage resources means that sensitive data may leak because data destruction policies may be impossible to implement
- Media cannot be physically destroyed when a customer change provider because a disk is still being used by another tenant
- Customer storage cannot be located or tracked as it moves through the cloud

Service Level Agreement

- Clauses with conflicting promises to different stakeholders
- Clauses may also be in conflict with promises made by other clauses or clauses from other providers.

Vulnerabilities

Audit or Certification Not Available to Customers

- The CP cannot provide any assurance to the customer via audit certification.
- Open source hypervisors or customized versions of them (e.g., Xen) may not have Common Criteria certification, etc

Certification Schemes Not Adapted to Cloud

- Very few if any cloud-specific control, which means that security vulnerabilities are likely to be missed.

Vulnerabilities

Storage of Data in Multiple Jurisdictions

- Mirroring data for delivery by edge networks and redundant storage without real-time information available to the customer of where data is stored

Lack of Information on Jurisdictions

- Data may be stored and/or processed in high risk jurisdictions where it is vulnerable to confiscation by forced entry.

Vulnerabilities

Lack of Cloud Security Awareness

- Cloud customers and providers are not aware of the risks they face when migrating into the cloud, particularly those risks that are due to cloud specific threats, i.e. loss of control on data, cloud provider lock-in, exhausted resources of the cloud provider.

Lack of Vetting Processes (Personel Background Checks)

- Since there may be very high privilege roles within cloud providers, due to the scale involved, the lack or inadequate vetting of the risk profile of staff with such roles is an important vulnerability

Unclear Roles and Responsibilities

- Inadequate definition of roles and responsibilities in the cloud provider organization

Vulnerabilities

Poor Enforcement of Role Definitions

- Within the cloud provider, a failure to segregate roles may lead to excessively privileged roles which can make extremely large systems vulnerable

Need-to-know Principle Not Applied

- Poorly defined roles and responsibilities
- Parties should not be given unnecessary access to data

Inadequate Security Procedures

- Lack of physical perimeter controls (smart card authentication at entry);
- Lack of electromagnetic shielding for critical assets
- Lack of policy for logs collection and retention
- Inadequate or misconfigured filtering resources

Os And Application Vulnerabilities

Mismanagement

- System or OS vulnerabilities
- Untrusted software
- Poor and untested business continuity and disaster recovery plan
- Incomplete or inaccurate asset inventory
- Poor or inadequate asset classification
- Unclear asset ownership

Application Vulnerabilities and Poor Patch Management

- Bugs in the application code
- Conflicting patching procedures between provider and customer
- Application of untested patches
- Vulnerabilities in browsers
- Dormant virtual machines
- Outdated virtual machine templates

Cloud security ;-)

Information-centric security with one of

- Untrusted infrastructure IaaS
- Untrusted Platform+Infrastructure PaaS
- Untrusted Software+Platform+Infrastructure SaaS

and a larger attack surface

Cloud Computing Threat Model (threat = what could go wrong)

ENISA

Cloud Computing Risk Assessment

Threat Model

Risk 1:	Resource Exhaustion
Risk 2:	Customer Isolation Failure
Risk 3:	Management Interface Compromise
Risk 4:	Interception of Data in Transmission
Risk 5:	Data leakage on Upload/Download, Intra-cloud
Risk 6:	Insecure or Ineffective Deletion of Data
Risk 7:	Distributed Denial of Service (DDoS)
Risk 8:	Economic Denial of Service
Risk 9:	Loss or Compromise of Encryption Keys
Risk 10:	Malicious Probes or Scans
Risk 11:	Compromise of Service Engine/Hypervisor
Risk 12:	Conflicts between customer hardening procedures and cloud environment

Threat Model

Risk 13:	Subpoena and E-Discovery
Risk 14:	Risk from Changes of Jurisdiction
Risk 15:	Licensing Risks
Risk 16:	Network Failure
Risk 17:	Networking Management
Risk 18:	Modification of Network Traffic
Risk 19:	Privilege Escalation
Risk 20:	Social Engineering Attacks
Risk 21:	Loss or Compromise of Operation Logs
Risk 22:	Loss or compromise of Security Logs
Risk 23:	Backups Lost or Stolen
Risk 23:	Unauthorized Access to Premises, Including Physical Access to Machines and Other Facilities
Risk 25:	Theft of Computer Equipment.

Threat Model

Risk 13:	Subpoena and E-Discovery
Risk 14:	Risk from Changes of Jurisdiction
Risk 15:	Licensing Risks
Risk 16:	Network Failure
Risk 17:	Networking Management
Risk 18:	Modification of Network Traffic
Risk 19:	Privilege Escalation
Risk 20:	Social Engineering Attacks
Risk 21:	Loss or Compromise of Operation Logs
Risk 22:	Loss or compromise of Security Logs
Risk 23:	Backups Lost or Stolen
Risk 23:	Unauthorized Access to Premises, Including Physical Access to Machines and Other Facilities
Risk 25:	Theft of Computer Equipment.

Threat Model Second Version

Policy Risk

- R.1 Lock-in
- R.2 Loss of governance
- R.3 Compliance challenges
- R.4 Loss of business reputation due to co-tenant activities
- R.5 Cloud service termination or failure
- R.6 Cloud provider acquisition
- R.7 Supply chain failure = awareness of this class of attacks is increasing due to some recent attacks. Very revealing situation, an old attack become critical when the customers learns it could occur

Threat Model Second Version

Technical risks

- R.8 Resource exhaustion (under or over provisioning)
- R.9 Isolation failure
- R.10 Cloud provider malicious insider - abuse of high privilege roles
- R.11 Management interface compromise (manipulation, availability of infrastructure)
- R.12 Intercepting data in transit
- R.13 Data leakage on up/download, intra-cloud
- R.14 Insecure or ineffective deletion of data
- R.15 Distributed denial of service (DDoS)
- R.16 Economic denial of service (EDOS)
- R.17 Loss of encryption keys
- R.18 Undertaking malicious probes or scans
- R.19 Compromise service engine
- R.20 Conflicts between customer hardening procedures and cloud environment

Threat Model Second Version

Legal risks

- R.21 Subpoena and e-discovery
- R.22 Risk from changes of jurisdiction
- R.23 Data protection risks
- R.24 Licensing risks

Threat Model Second Version

Risks not specific to the cloud

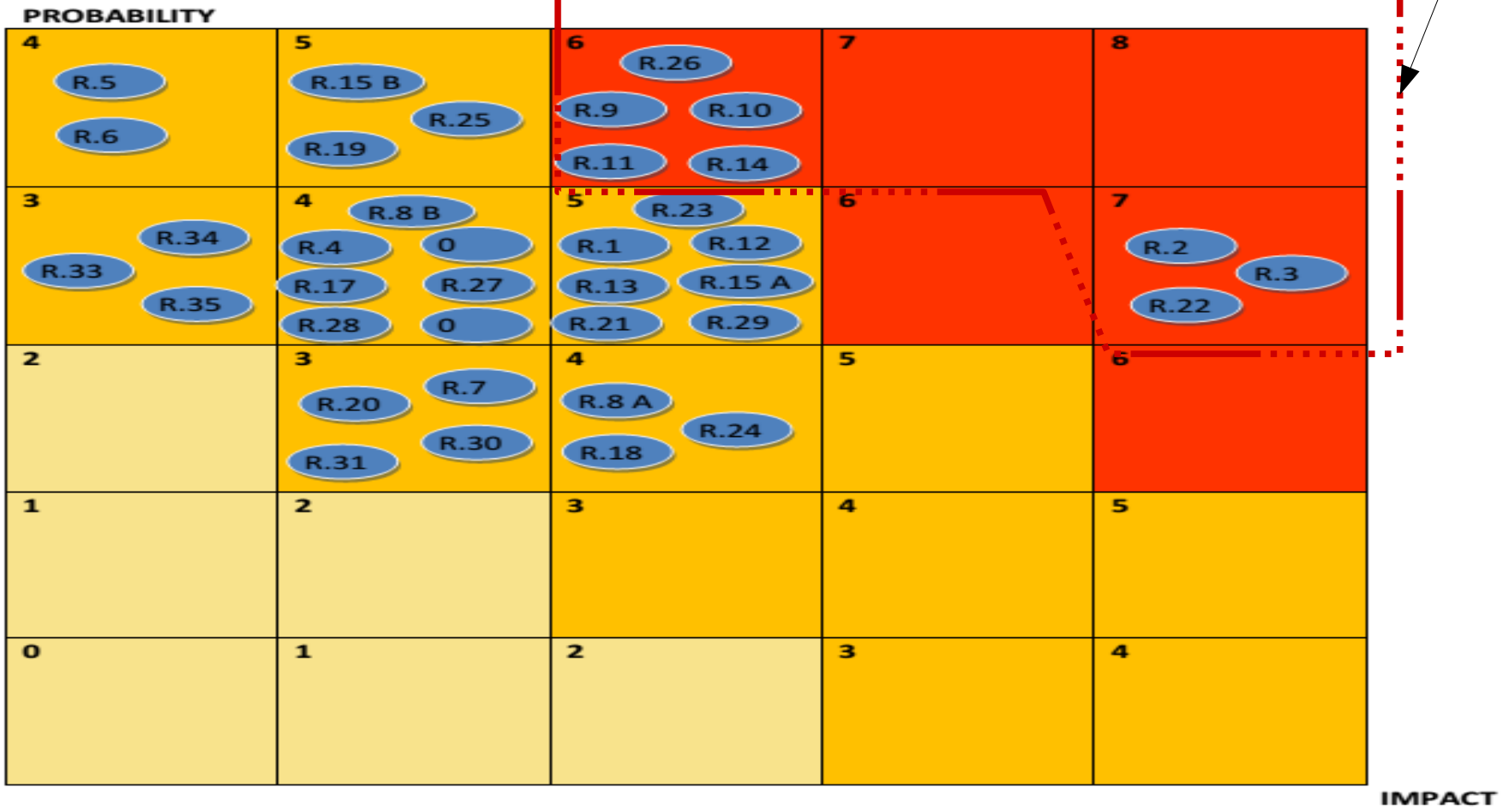
- R.25 Network breaks
- R.26 Network management (ie, congestion / non-optimal use)
- R.27 Modifying network traffic
- R.28 Privilege escalation
- R.29 Social engineering attacks (ie, impersonation)
- R.30 Loss or compromise of operational logs
- R.31 Loss or compromise of security logs (manipulation of forensic investigation)
- R.32 Backups lost, stolen
- R.33 Unauthorized access to premises (including physical access to machines and other facilities)
- R.34 Theft of computer equipment
- R.35 Natural disasters

Risk Assessment using a Risk Matrix

	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

Risk Assessment

most dangerous are related to the provider



Risk Assessment: top risks

R.2	Loss of governance
R.3	Compliance challenges
R.9	Isolation failure
R.10	Cloud provider malicious insider - abuse of high privilege roles
R.11	Management interface compromise (manipulation, availability of infrastructure)
R.14	Insecure or ineffective deletion of data
R.22	Risk from changes of jurisdiction
R.26	Network management (ie, congestion / non-optimal use)

SME moving to a cloud: opportunities (ENISA)

Network and information security opportunities
O1: Geographic spread
O2: Elasticity
O3: Standard formats and interfaces
O4: Physical security
O5: Incident response around-the-clock
O6: Software development
O7: Patching and updating
O8: Backups
O9: Server-side storage
O10: Security-as-a-service and security add-ons
O11: Certification and compliance

SME moving to a cloud: threats (ENISA)

Network and information security risks
R1: Software security vulnerabilities
R2: Network attacks
R3: Social engineering attacks
R4: Management GUI and API compromise
R5: Device theft/loss
R6: Physical hazards
R7: Overloads
R8: Unexpected costs
R9: Vendor lock-in
R10: Administrative or legal outages
R11: Foreign jurisdiction issues

In the following...

- We will focus on technical risks and in some risks related to the provider
- A typical risk is the failure of isolation or the abuse of roles by the insider (working for the cloud provider)