

ICT Risk Assessment (and Management) (of networks+Cloud Computing+IOT+ ...)

Fabrizio Baiardi
f.baiardi@unipi.it



Why this course ... :-)

Any logical structure that humans can conceive will be susceptible to attacks, and the more complex the structure, the more certain that it can be attacked

John Mc Afee speaking about the defects in AI software

If you don't know how "it" works then you won't manage its risks. Or, as they say in the poker world, if after ten minutes at the table you don't know who the patsy is—you're the patsy.

Daniel E. Geer, Jr.



Syllabus

- Introduction to ICT Security
 - Risk Analysis
 - Countermeasures
- Cloud Computing:
 - Supporting Technologies
 - Virtualization
 - Elasticity
 - Properties and Rules
 - Security of Cloud Computing
 - Threat Model
 - Attacks (Classic + Spectre...)
 - Countermeasures
- IOT

Fully general

Clouds are interesting!!!

The course structure is updated according to

- new vulnerabilities
- new attacks



Exam

One of

- Written test :-(
 - Project work (even in a group)
- Tool: You choose a security tool
 - You read the documentation
 - You run some experiments
 - You prepare a relation
- Lecture: You choose a topic
 - You choose some papers (ACM, IEEE..)
 - You prepare the slide
 - You present your lecture



Exam

Material

- Slides:

<https://elearning.di.unipi.it/course/view.php?id=217>

- Book: Security Engineering (Ross Anderson, free book)

<https://www.cl.cam.ac.uk/~rja14/book.html>

IOT and Cloud are related

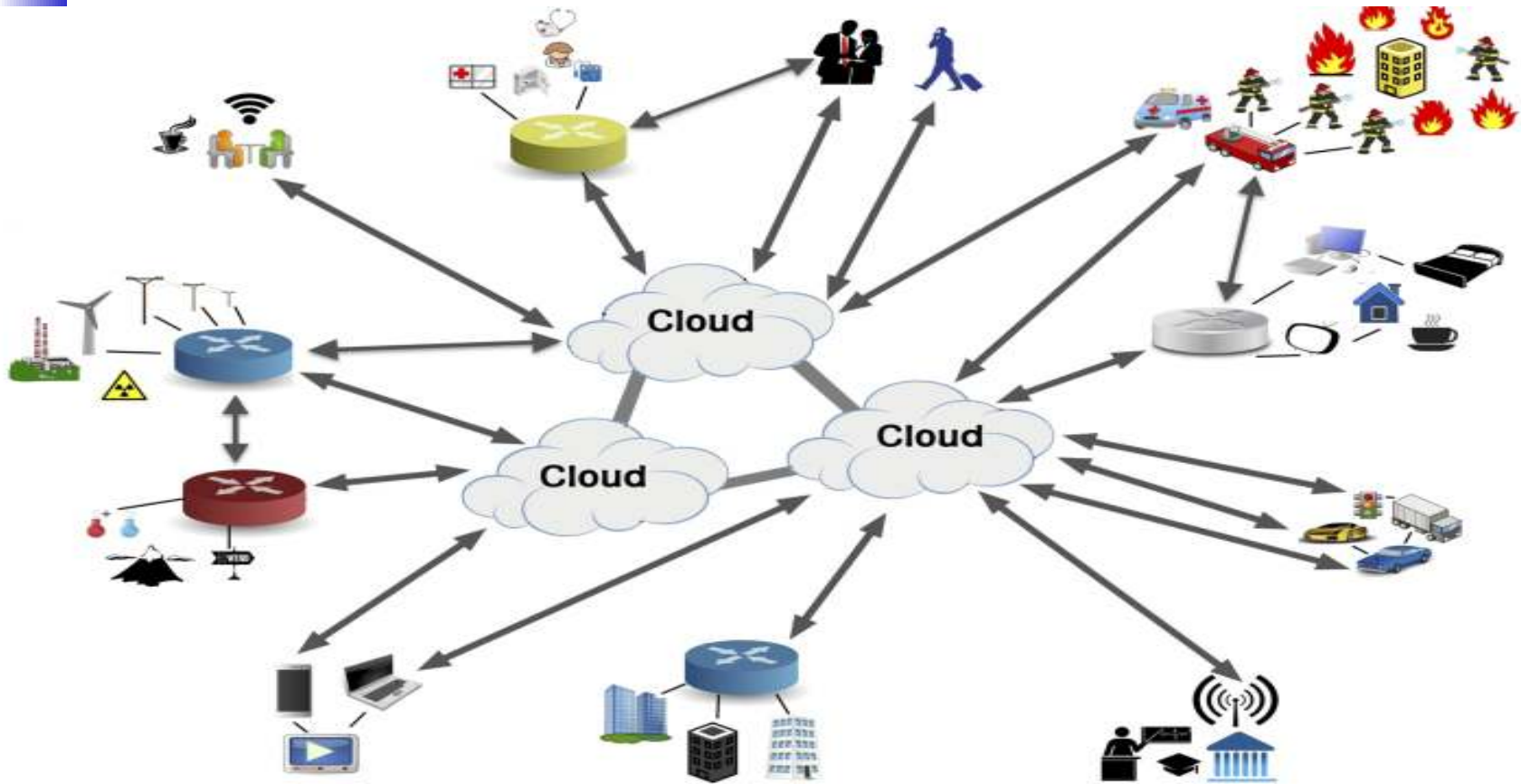
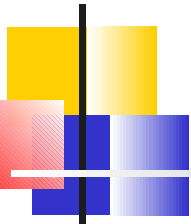


Fig. 1. An illustration of IoT including cloud services (IoT-Cloud).

The beginning of “Cloud Computing”

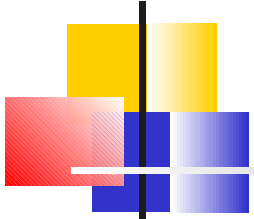


- John McCarthy opined that “Computing may someday be organized as a public utility”

John McCarthy, MIT Centennial in 1961

- “Comes from the early days of the Internet where we drew the network as a cloud... we didn’t care where the messages went... the cloud hid it from us” – Kevin Marks, Google
- First cloud around networking (TCP/IP abstraction)
- Second cloud around documents (WWW data abstraction)
- The emerging cloud hides details to final users by abstracting infrastructure complexities of servers, applications, data, and heterogeneous platforms

Utility vs Cloud Computing

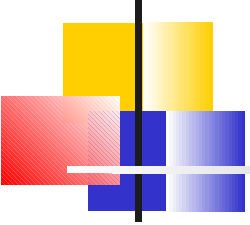


Utility computing

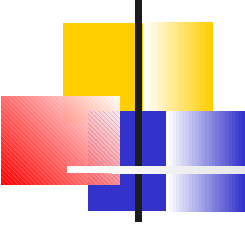
- customers receive computing resources from a service provider (hw and/or sw) and “pay by the drink,” as for electric service at home
- equires a cloud-like infrastructure
- focused on better economics. Corporate data centers are usually underutilized, with resources often idle = overprovisioning = more hardware to handle peaks
- allows companies to only pay for the computing resources they need, when they need them.

Cloud computing is a broader concept that relates to the underlying architecture where services are designed. It may be applied equally to utility services and internal corporate data center

Fog vs Cloud Computing

- 
-
- Fog Computing extends Cloud computing and services to the network edge. It is characterized by proximity to end-users, dense geographical distribution, and mobility support. Services are hosted at the network edge or even end devices such as set-top-boxes or access points.
 - Fog Computing
 - can reduce service latency and improve QoS, resulting in superior user-experience.
 - supports emerging Internet of Everything (IoE) that demand real-time/predictable latency
 - Geographically distributes devices over heterogeneous platforms, spanning multiple management domains

A Working Definition of Cloud Computing



Cloud computing is a model for enabling

- convenient,
- On-demand
-

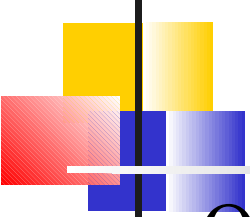
network access to a shared pool of configurable and geographically distributed resources (e.g., networks, servers, storage, applications,) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

This cloud model promotes availability and is defined in terms of

five essential **characteristics**,
three **service models**,
four **deployment models**.

Design space

5 Essential Cloud Characteristics

- 
-
- On-demand self-service
 - Broad network access = web access
 - Resource pooling = Location independence through web / broad band access
 - Rapid elasticity
 - Measured service

Cloud computing is possible only because of web+broadband and it is not available if/when/where internet access is not available

Common Cloud Characteristics

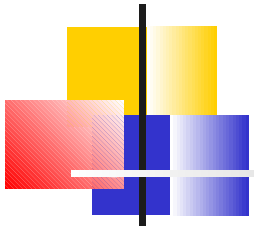
- 
-
- Massive scale
 - Homogeneity
 - Virtualization
 - Resilient and elastic computing
 - Low cost software
 - Geographic distribution
 - Service orientation
 - Advanced security technologies



NIST framework and terms

- This course adopts and follows a framework developed by the National Institute of Standard and Technologies
- This framework has been and is used in the USA to drive the adoption of cloud computing in federal and state offices
- Focused on
 - the kind of access to the cloud system (service model)
 - the underlying architecture (deployment model)

The NIST Cloud Definition Framework



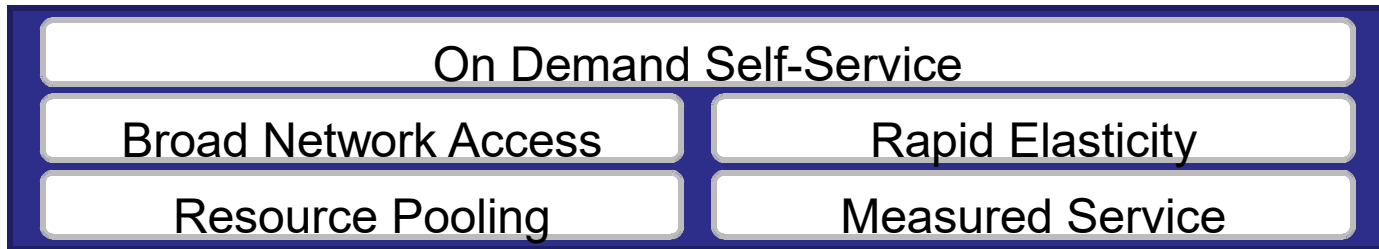
Deployment Models



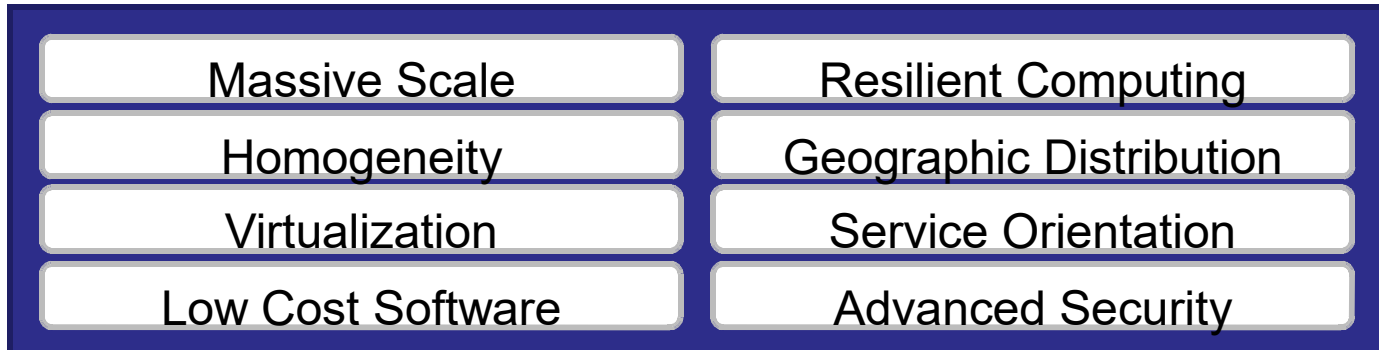
Service Models

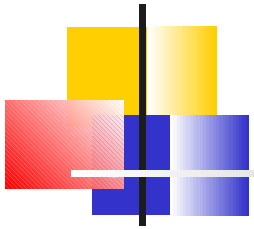


Essential Characteristics



Common Characteristics





Cloud and Security - I

Economy and flexibility



**Private
Cloud**

**Community
Cloud**

Public Cloud

Software as a
Service (SaaS)

Platform as a
Service (PaaS)

Infrastructure as a
Service (IaaS)



Economy and flexibility



Cloud and Security - II

Complexity of security problems



**Private
Cloud**

Software as a
Service (SaaS)

**Community
Cloud**

Platform as a
Service (PaaS)

Public Cloud

Infrastructure as a
Service (IaaS)



Complexity of security problems



IOT

"The Internet of Things (IoT) is the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure. Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers a variety of protocols, domains, and applications. Things, in the IoT, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, automobiles with built-in sensors, or field operation devices that assist fire-fighters in search and rescue." Wikipedia

- *IoT network resilience to cyber attacks*
- *Individual as a Data cluster*
- *Privacy*
- *Concrete cyber threats*
- *Influencing human behavior*





IOT = Smart Thing

- Anything that is “smart” is smart because it has a computer and the computer can be attacked
- An important component of the IOT are sensors
- Several attacks against sensors exploit the physics a sensor exploits
 - attacks using ultrasound against a microphone
 - attacks sending fake information to GPS sensors
 - ...

Complexity of security increases because of the lack of computational resources in the computer



ICT Security & Risk

- A topic at the intersection of three areas
 - Computer Science
 - Human Resources and Management
 - Economy
- From security to risk assessment and management
- “Kids speaks about security real women/men about risk assessment and management ” economy is involved
- $\text{Risk} = \text{Risk}(\text{probability, damage (or impact)})$
- Risk management = an approach strongly related to probability, impact, cost effectiveness of solutions



ICT Security & Risk

Largest risks in these years

	Likelihood*	Impact**	Risk score
Cyber attack & data breach	3.25	2.17	7.05
IT and telecom outage	3.12	1.91	5.95
Adverse weather/natural disaster (e.g. hurricane/earthquake)	3.01	1.82	5.47
Critical infrastructure failure	2.48	2.19	5.43
Reputation incident	2.53	2.02	5.11
Regulatory changes	2.95	1.63	4.80
Lack of talent/key skills	2.73	1.68	4.58
Supply chain disruption	2.5	1.78	4.45
Interruption to utility supply	2.67	1.65	4.40
Political change	2.66	1.58	4.20
Introduction of new technology (Blockchain, AI, IoT)	2.63	1.57	4.12
Health and safety incident	2.69	1.53	4.11
Lone attacker/active shooter incident	1.71	2.32	3.96
Exchange rate volatility	2.31	1.57	3.62
Disease outbreak	2.01	1.7	3.41
Higher cost of borrowing	2.1	1.48	3.10
Political violence/civil unrest	1.96	1.55	3.03
Product quality incident/product recall	1.83	1.6	2.92
Natural resources shortage	1.75	1.54	2.69



Why cybersec matters

- Any organization strongly depends upon
 - Its private ICT resources
 - The ICT resources of its partners
 - The ICT systems that connect its private resources with the partners' resources
- Any organization should be able to prove to other ones that it controls its ICT resources
- Security = the owner controls the resources
- Anytime an organization has to prove that it satisfies some standards (not only ICT ones) it has to prove it controls its ICT resources



Why cybersec matters



Mark Andreessen

founder of Netscape,
renowned Venture Capitalist
Andreessen-Horowitz

Software is eating the
world, in all sectors

In the future every
company will become a
software company



Information Security: the triad

- **Confidentiality**
An information can be read only by those that are entitled
- **Integrity**
An information can be updated only by those that are entitled
- **Availability**
An information can be read and updated by those that are entitled when they require the operation. An ICT resource should be available to those that are entitled to use it



Other properties

- Authentication = you are who you say you are
- Tracing = who has invoked an operation
- Accountability = pay for what you have used
- Auditability = evaluate the effectiveness of security solutions
- Forensics = information to prove that some laws have been violated (authentication + integrity)
- Privacy = protection of personal information (stronger than the triad, no inference)



Vulnerability

- A first key concept for security
- A vulnerability is a defect (an error, a bug) in a person, a component, a set of rules that makes it possible to violate a security property = a bug that enables an attack
- While all vulnerabilities are bugs (errors...) not all bugs are vulnerabilities



Threat agent

- A second key concept for security
- A source of attacks = actions that exploits vulnerabilities to violate some security property
- An agent may be natural (flooding, earthquake) or man-made
- Man-made may be random or malicious
- We can assess risk only if we know both vulnerabilities and threat agents for a system

Intrusion against an ICT system



- An intrusion is a sequence of actions and attacks to (illegally) control of (a subset of) an ICT system
- A program can implement some actions (exploit)
- Each attack is possible because of vulnerabilities (defect) of the target system or of its users
- Who controls an ICT (sub)system can
 - Collect any information in the (sub)system
 - Update any information in the (sub)system
 - Prevent someone from accessing any resource/information in the (sub)system



Our perspective

- Adversary focused= a cost effective defense from adversaries and their attacks against an ICT system
- Why/Which/When attacks may be successful
- The actions and the strategy of an attacker (adversary)
- How much work is required to attack
- How the risk due to attacks can be managed (prevented, reduce their frequency or their impact ...)
- Selection, evaluation and deployment of cost effective countermeasures (changes to the system)
- Cost, return, investment,