TSC

Cloud Technologies and Systems
Class 05

Carlos Coutinho

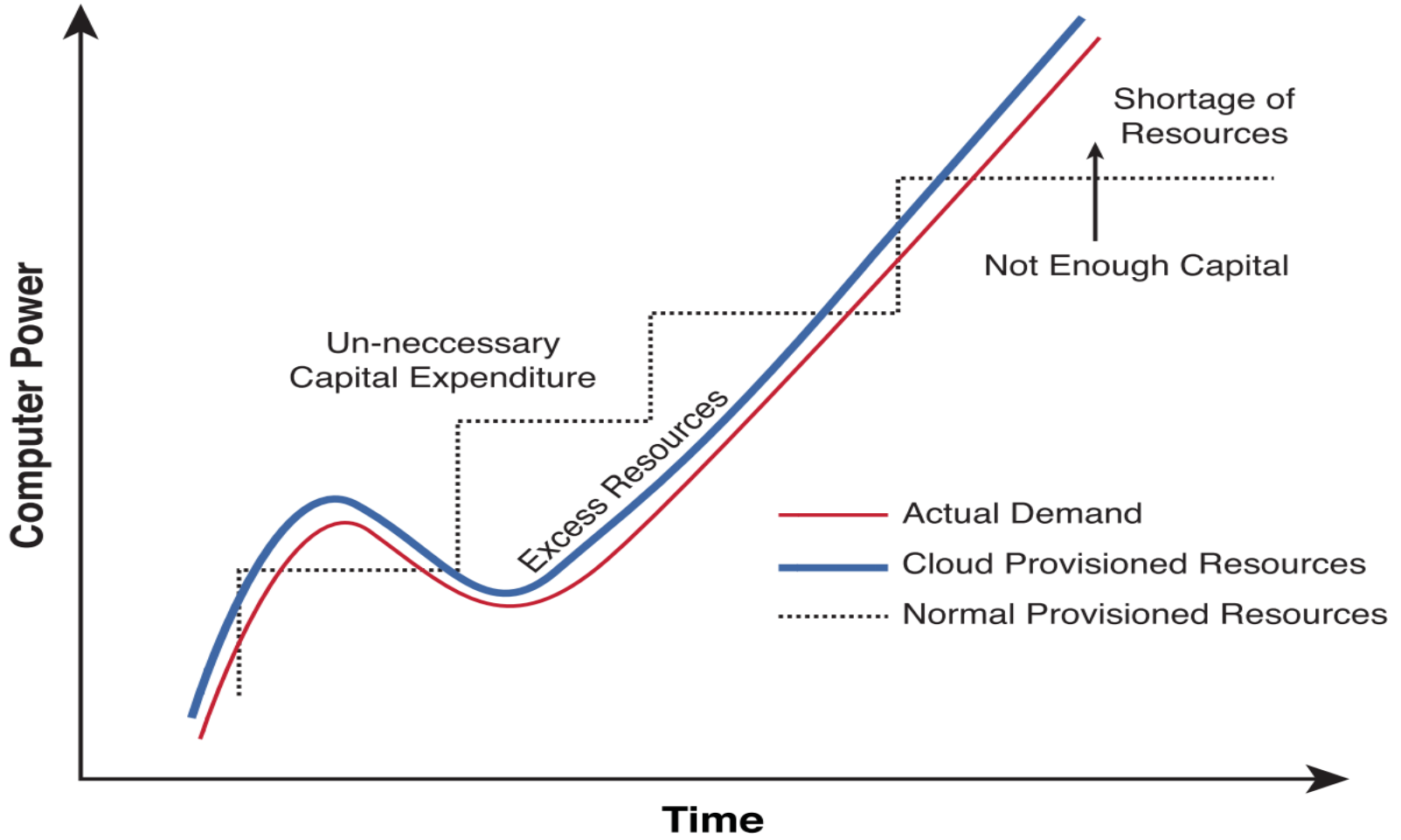
Topics

- Summary Cloud Concepts
- Cloud Pros & Cons
- Cloud Service Types
- Cloud Deployment Models
- Security
- Security Mechanisms

Terminology – Cloud Environment

- Highly **extensive infrastructure**
- Provides **pools** of IT **resources**
- Resources can be leased by **pay-for-use** model
- Only the **actual usage** of resources is **billed**
- Allows **accommodation** of usage **fluctuations**
- **Upscaling** and **Downscaling**
- High availability and QoS

Cloud ROI



Source: https://aws.amazon.com/economics

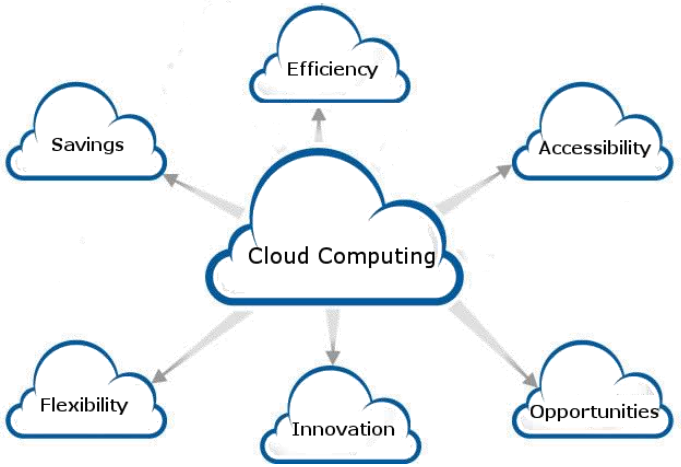
Cloud Computing

Advantages:

- Simplicity
- Cost Savings
- Efficiency
- Security

Cloud Computing

- Pros:
  - **Low CAPEX** investment in infrastructure
  - **Independence** on the **location** of the client
  - High **availability**, **scalability** and **elasticity**
  - **Resource abstraction** and ease of use
  - Resource **virtualisation**
  - **Pay-per-use** costs

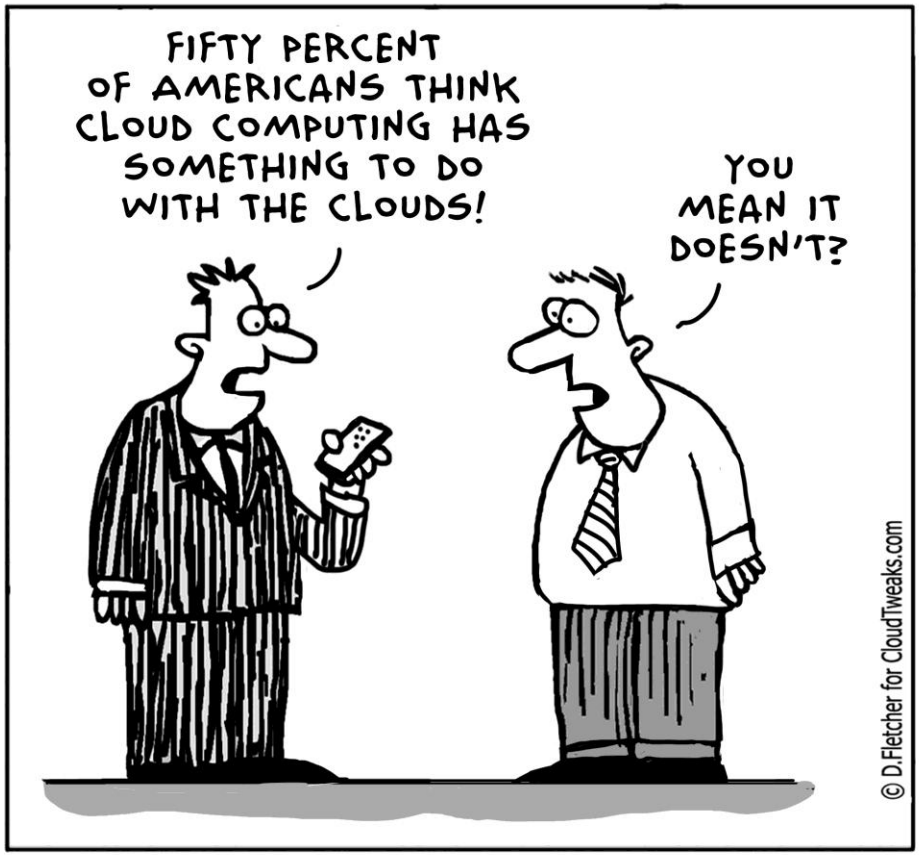


Cloud Computing

- Cons:
  - Strong **dependency** on the **Internet**
  - Failure may occur on data recovery
  - Security **vulnerabilities** to hackers
  - Very specific **regulations** on **privacy** and **security**
  - **Limited customisation** of services on Public Clouds

Cloud-Related Definitions

- **Lock-in**: When there is a significant cost to move from one cloud vendor to another
- **Portability**: Ability to move applications, data, tools from one cloud to another
- **Interoperability**: Ability of different clouds to interact together, e.g., communication
- **Federation**: Act of combining services from various cloud providers to provide a solution



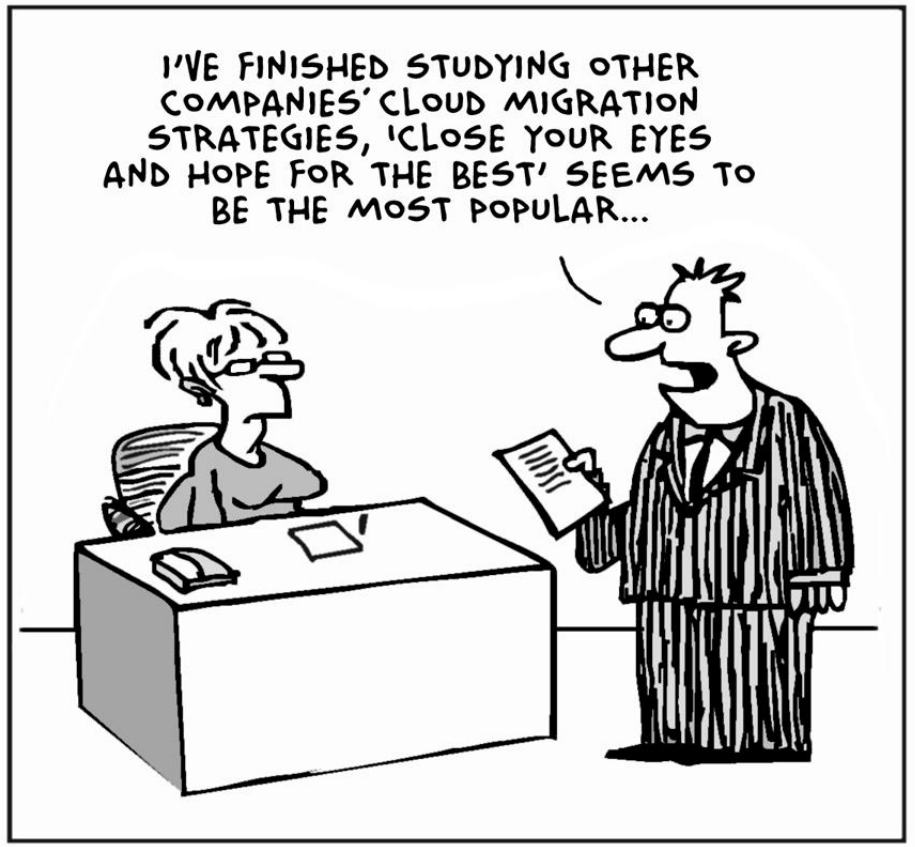
Cloud Computing

Concerns to adopt public clouds (adoption barriers):

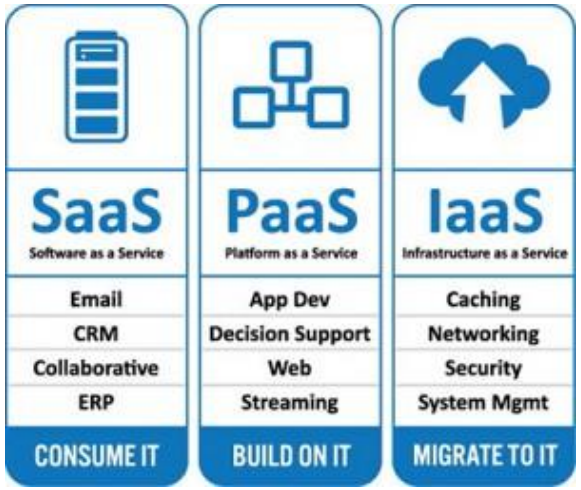
- **How** will the cloud keep **data secure** and available?
- How to comply with current and future **security & risk**?
- What type of **security services** are available?
- How to perform internal and external **audits** of security?
- How to **automate** resource **provisioning**?
- How to do on-demand **provisioning** in near **real time**?
- How to **orchestrate** new cloud tools and existing **legacy**?

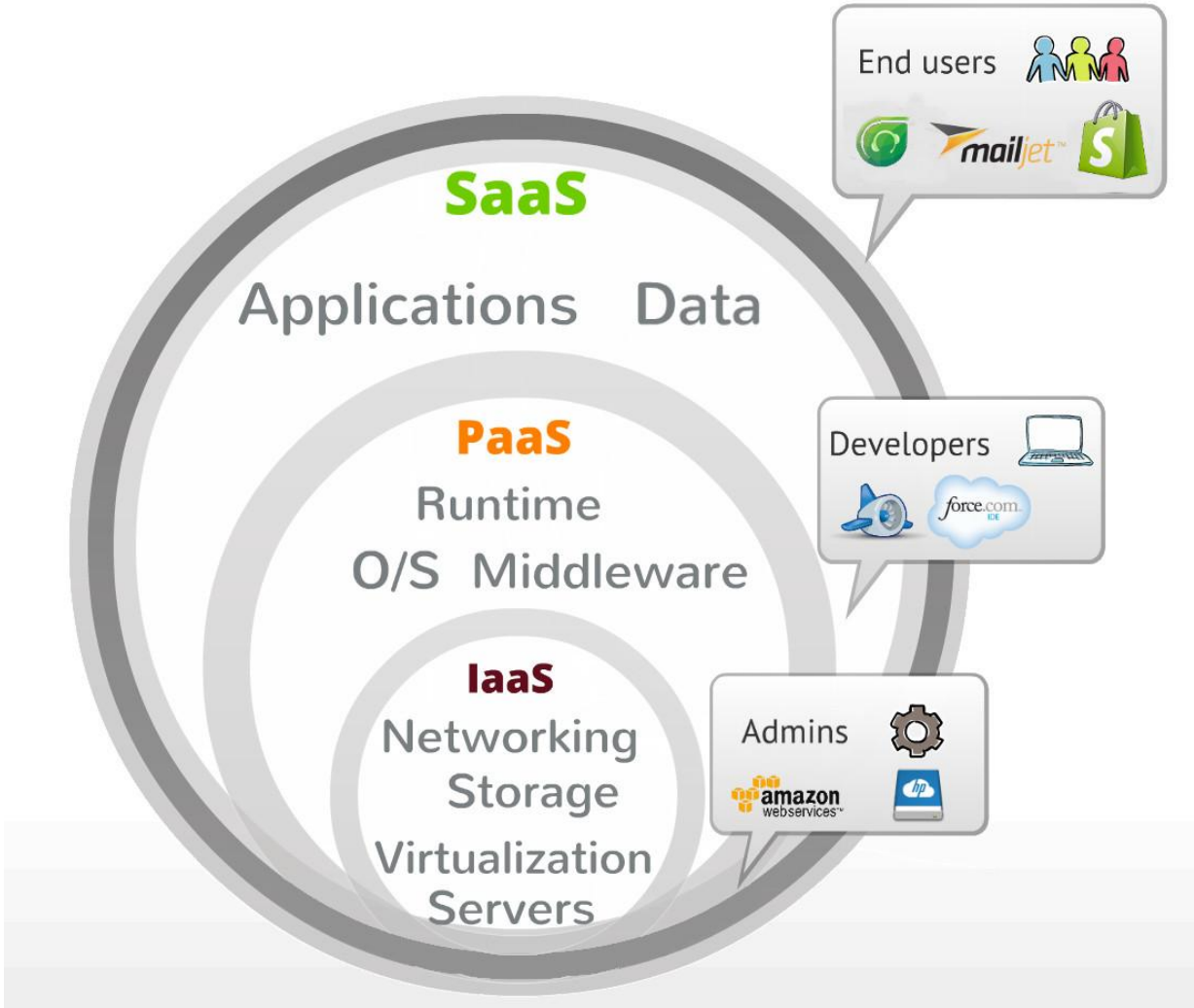
Cloud Migration Concerns

- Organisation adaptation
- Choosing from Service **Portfolio**
- Changing **Processes**
- Different Technology **Architecture**
- SLA **Management**
- Cloud Supplier **Management**
- Cloud Solution Governance

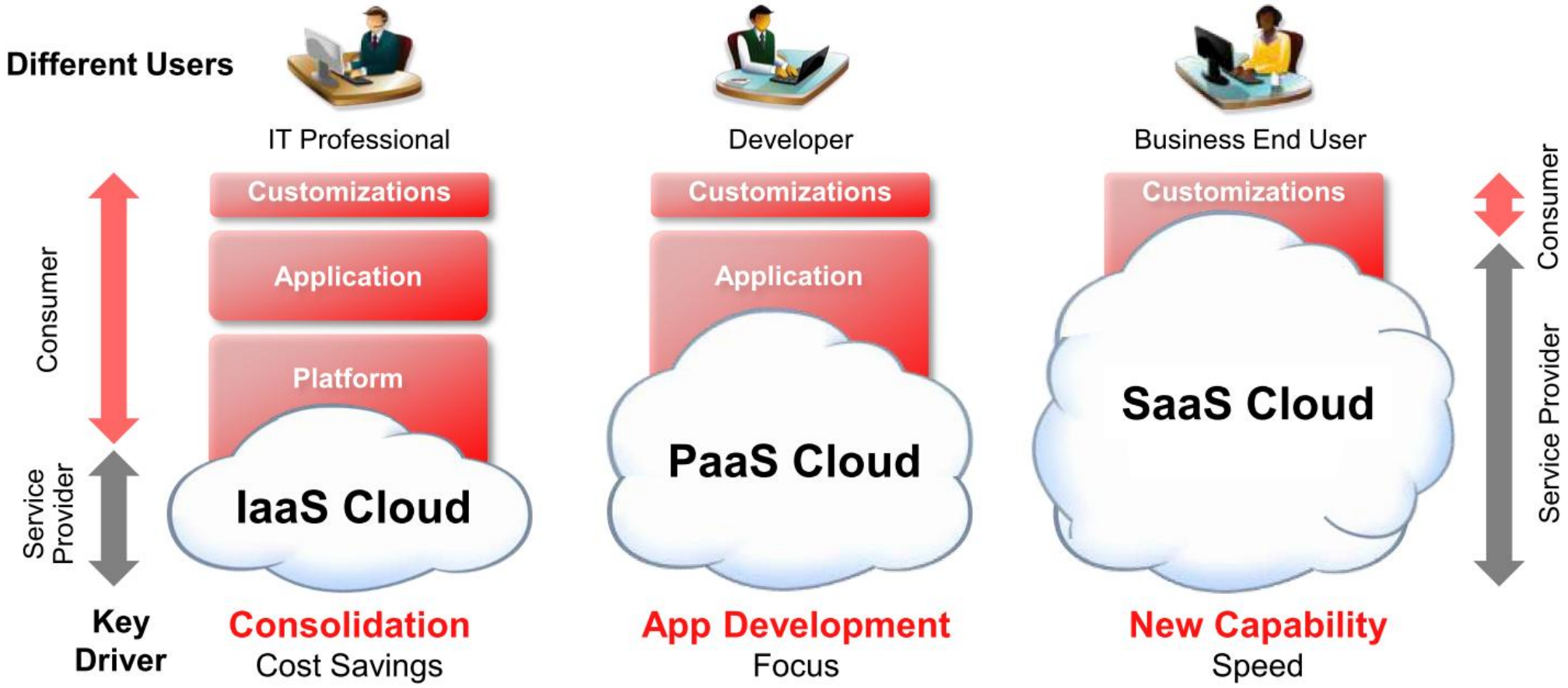


Cloud Service Types

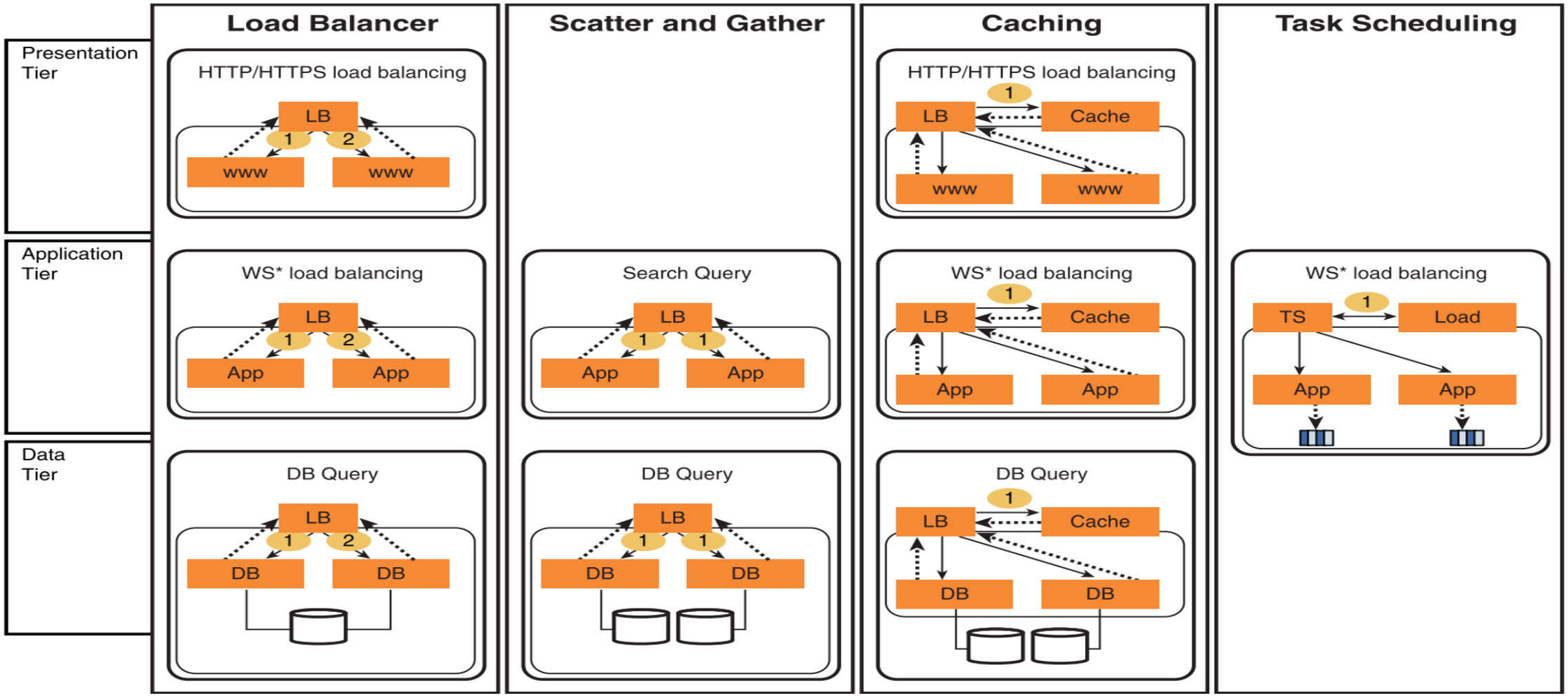




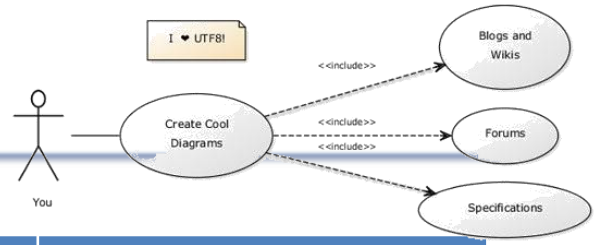
Cloud Service Types



Cloud Design Patterns – for performance

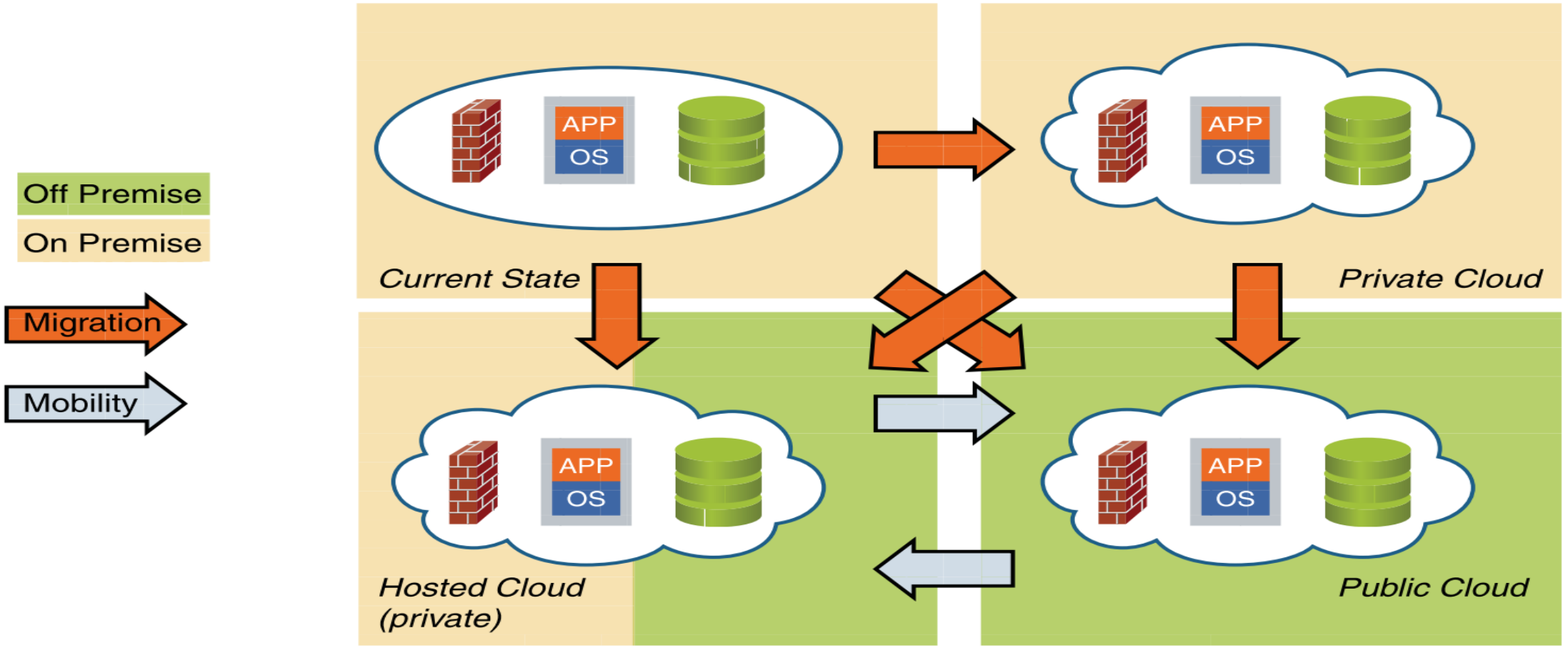


Cloud Use Cases



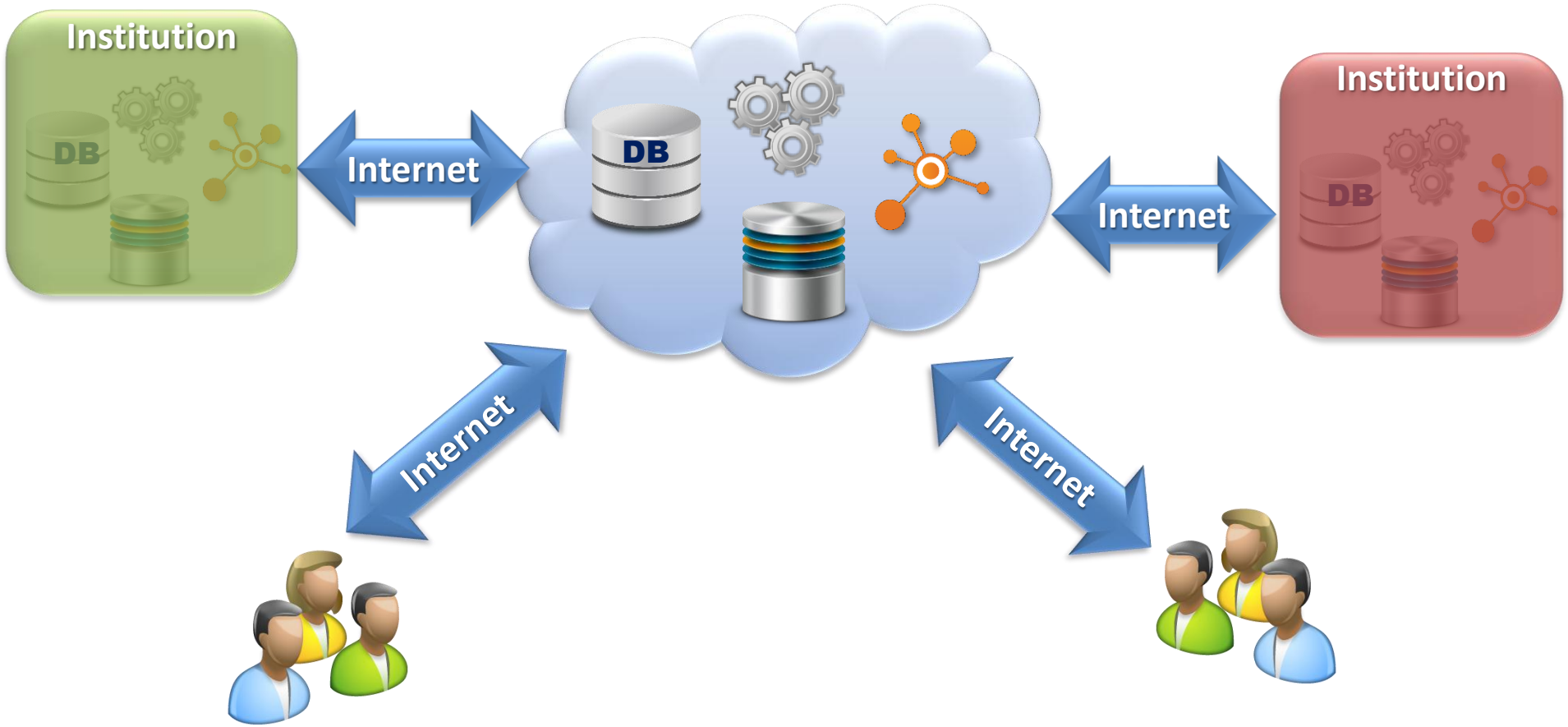
Use Case	Reasons for Moving to the Cloud	Service Models
Development and Test	Mobility, Distributed teams, cyclical usage	IaaS, PaaS
Business Continuity	High criticality, low usage	SaaS, IaaS
Usage Monitoring	Cloud platforms already have mechanisms for usage monitoring and cost allocation	IaaS
Desktop Management	Automated desktop delivery and management / thin clients	IaaS
Storage	Low utilization	IaaS
Compute-on-Demand	procurement waiting time, hardware subuse, and VM sprawl	IaaS

Cloud Deployment Models



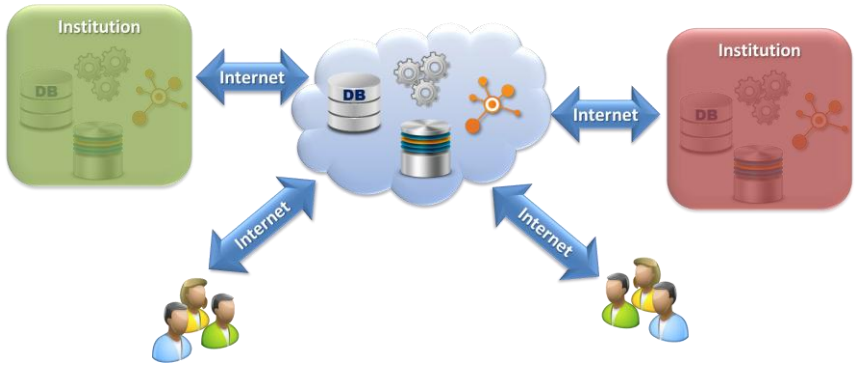
Cloud Computing

Public Cloud (e.g., Microsoft, Amazon, Google)



Cloud Computing

- **Public Cloud** (e.g., Microsoft, Amazon, Google)
  - **Multi-tenant**: customers buy server slices
  - Utility Model: **pay-as-you-go**, no contracts
  - **Shared Resources**: Special requirements not allowed
  - Partial control of Performance (add resources) + **SLA**
  - Self-managed



Cloud Computing

Concerns:

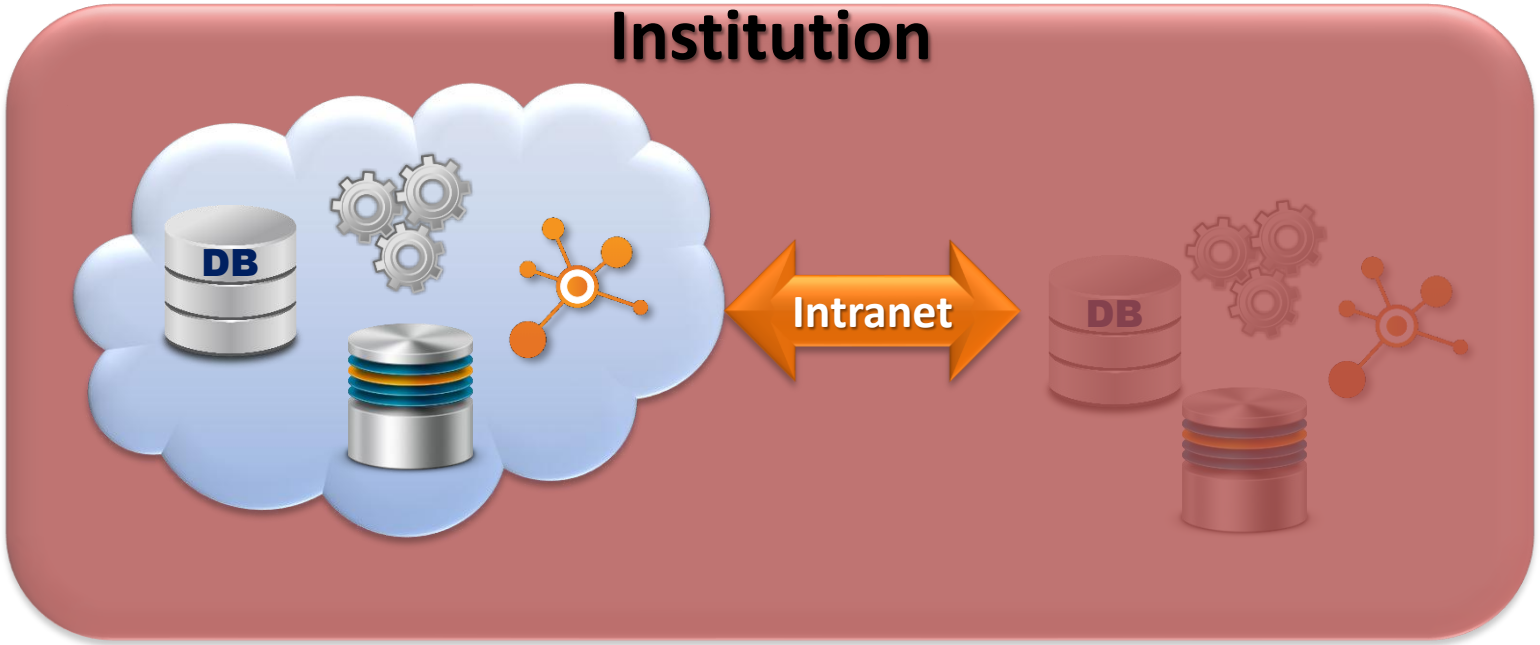
- Vendor Lock-in (early days)

https://www.bmc.com/blogs/vendor-lock-in/

- Security
- Integration
- ...

Cloud Computing

- **Private Cloud** (e.g., NASA, CERN)



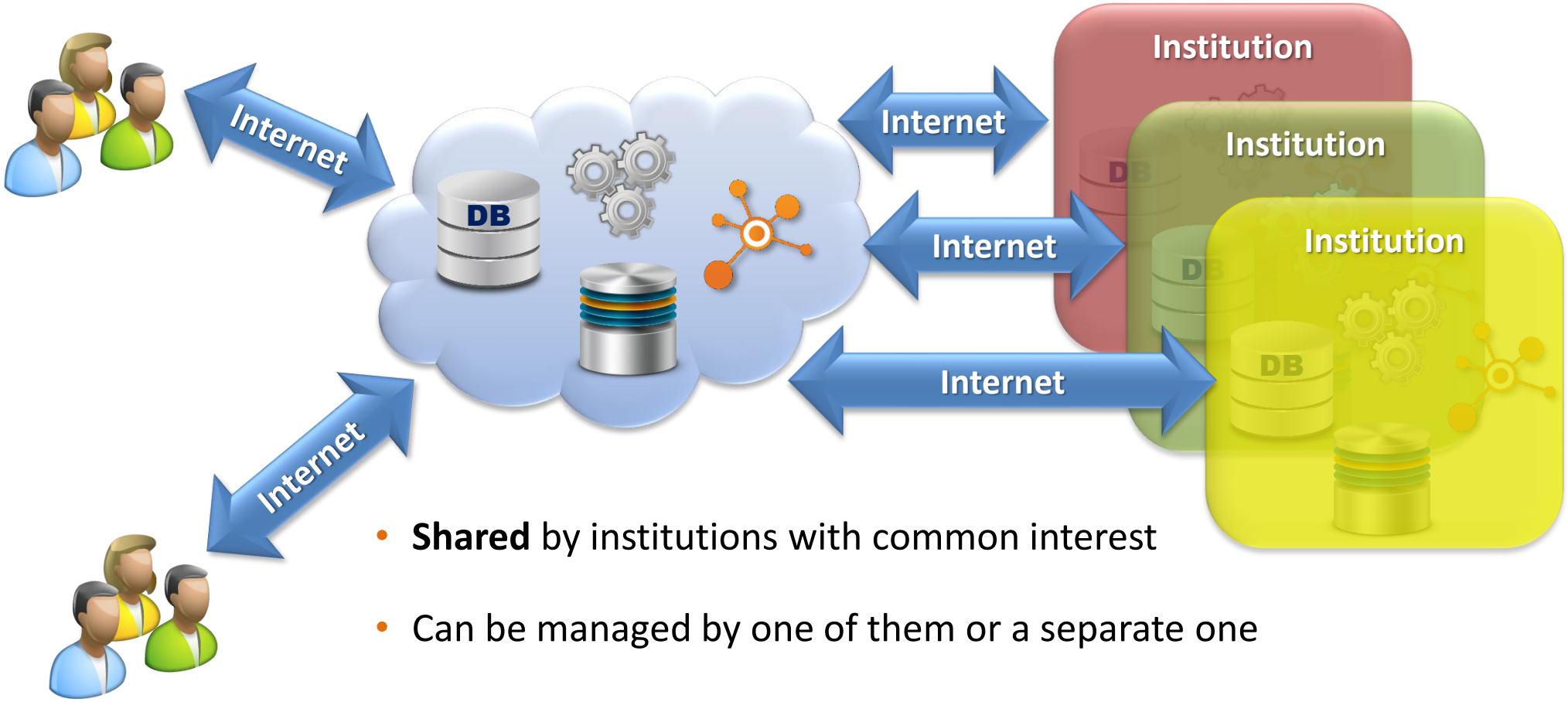
Cloud Computing

Private Cloud (e.g., NASA, CERN)

- **Single-tenant**: Resources dedicated to single customer
- **Security: Major concern**
- **Compliance norms** (e.g., SOC, PCI DSS)
- **Customisable** performance
- Hybrid deployments: **Integration of local HW**
- Virtualisation or not(Increased cost)
- **Fully-managed** solution

Cloud Computing

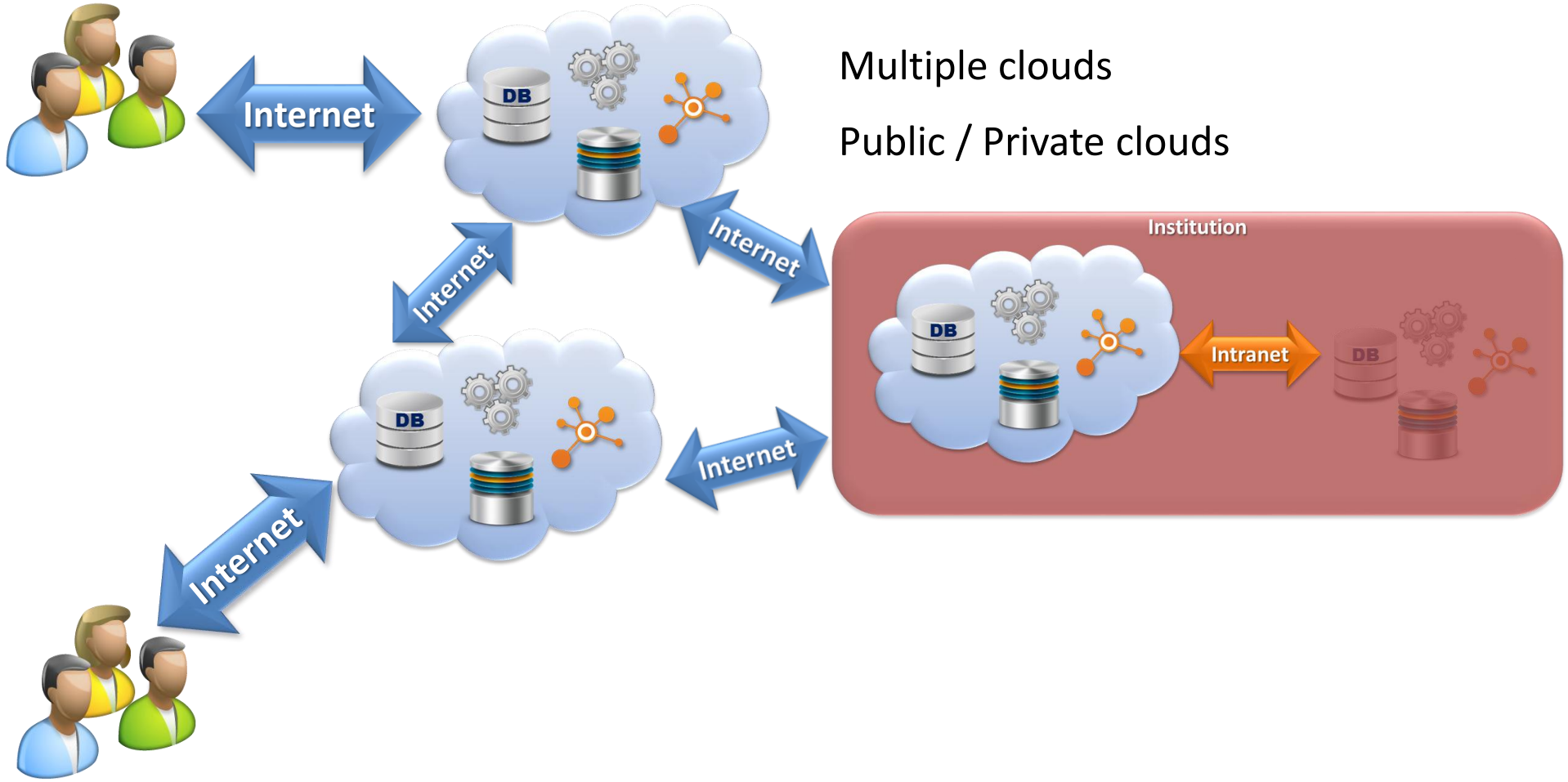
Community Cloud



- **Shared** by institutions with common interest
- Can be managed by one of them or a separate one

Cloud Computing

- **Hybrid Cloud**



Multiple clouds

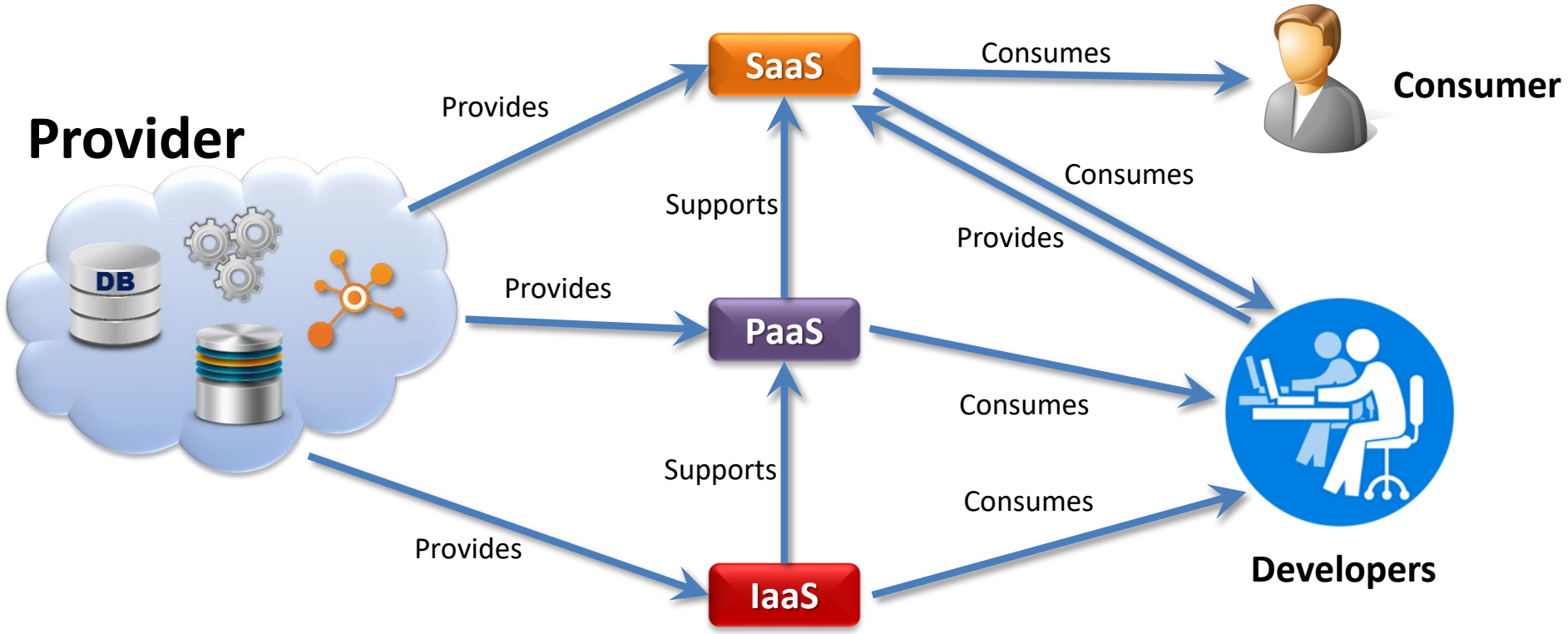
Public / Private clouds

Cloud Deployment Models

	Public	Private	Hosted (Private)
Access	Internet-connected Data centres/private IP-VPN	Corporate data centre	Internet-connected data centres/ corporate
Tenancy model	Multiple clients	Single company	Single company
Infrastructure type	Shared infrastructure	Dedicated infrastructure	Shared and dedicated Infrastructure (shared:facilities,network,…) (dedicated: servers)
Security model	Common across all customers, with Limited configurability	Unique to the customer	Based on the infrastructure type Contracted with the provider
Cloud manager	Provider	IT ops	Provider or/and IT ops
Billed by	Consumption	Consumption-based metering for Business Unit chargeback or Allocation	Monthly for dedicated infrastructure; excess billed by consumption

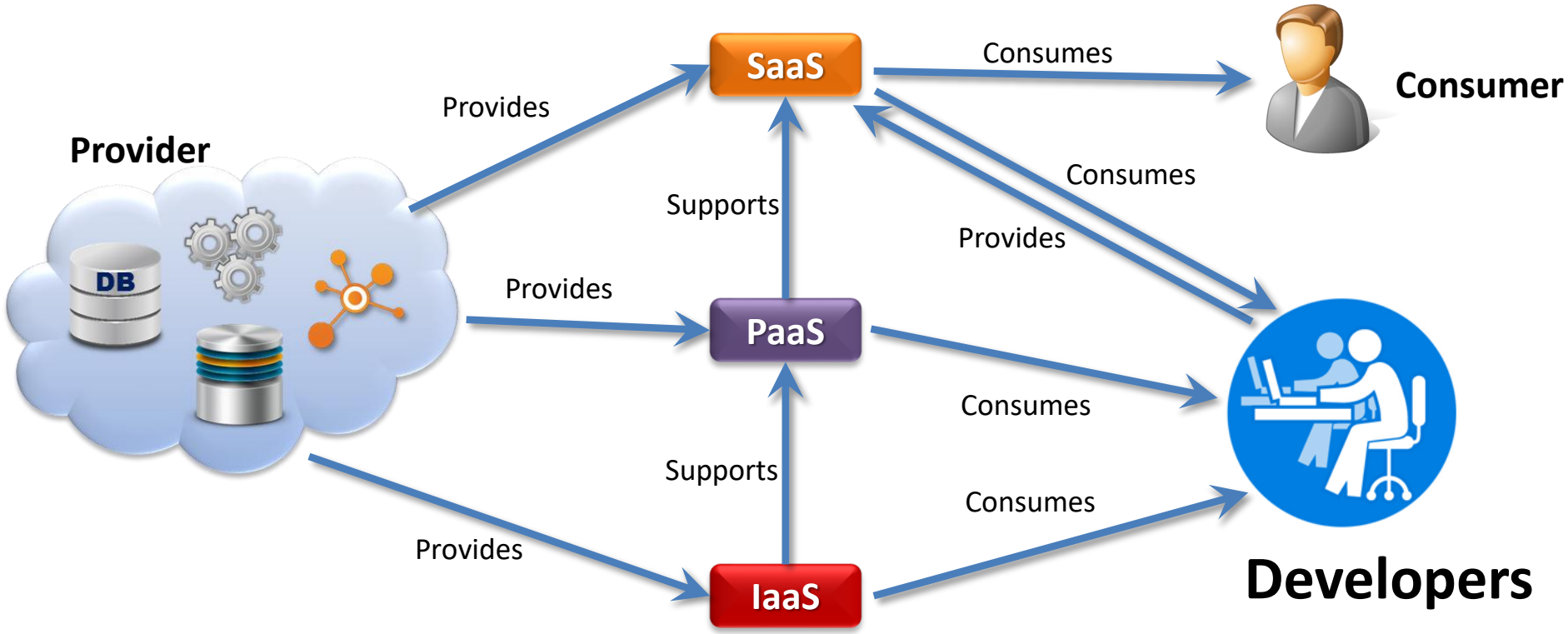
Cloud Roles - Provider

- Responsible for the **management** of all service layers
- **Maintains** infrastructure, installation and updates



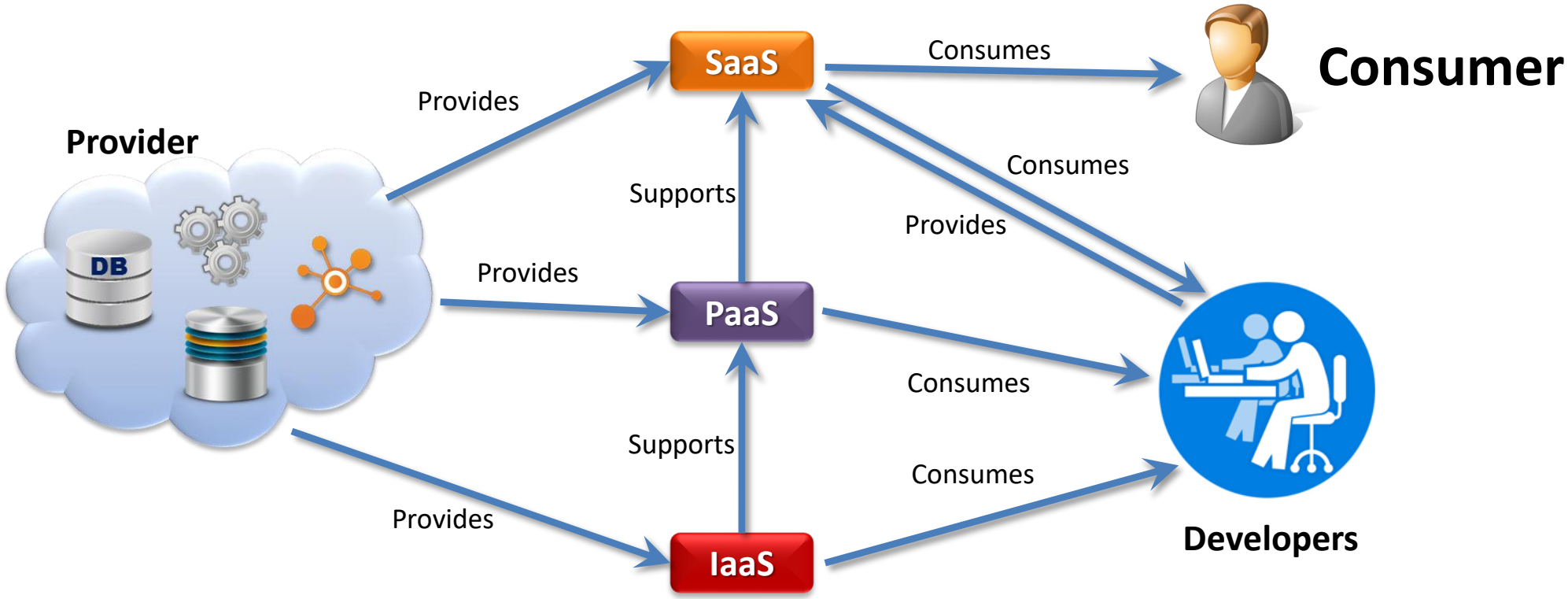
Cloud Roles - Developers

- **Produce** SaaS applications (generally)
- **Develop** SaaS based on IaaS, PaaS and SaaS



Cloud Roles - Consumer

- **Consumes** Services developed by Developers and provided by Providers
- Can be a **single individual** or an **organisation**



Infrastructure as a Service

IaaS

- **VM as a Service types**:
  - Persistent VMs
  - Non-persistent VMs

Infrastructure as a Service

IaaS

- **VM as a Service examples**:
  - Google Compute Engine
  - Microsoft Azure
  - Amazon EC2 (Elastic Compute Cloud)

Infrastructure as a Service

IaaS

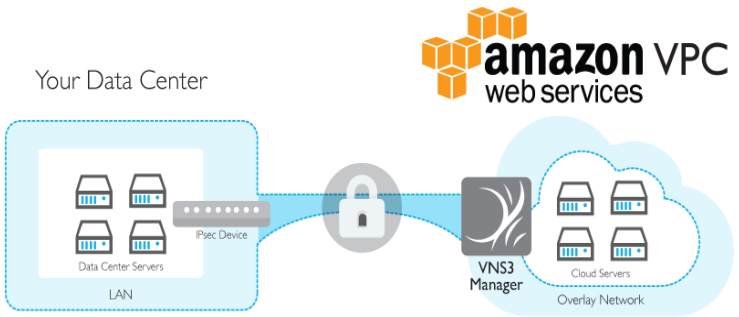
- **Storage as a Service**:
  - Google Cloud Storage
  - Microsoft Azure Storage

  - Amazon S3 (Simple Storage Service)

Infrastructure as a Service

IaaS

- **Virtual Network as a Service**:
  - Google Compute Engine
  - Microsoft Azure
  - Amazon VPC (Virtual Private Cloud)



Infrastructure as a Service

IaaS

- **SQL DBMS as a Service**:
  - Google Cloud SQL
  - Microsoft SQL Database
  - Amazon RDS (Relational Database Service)

Infrastructure as a Service

IaaS

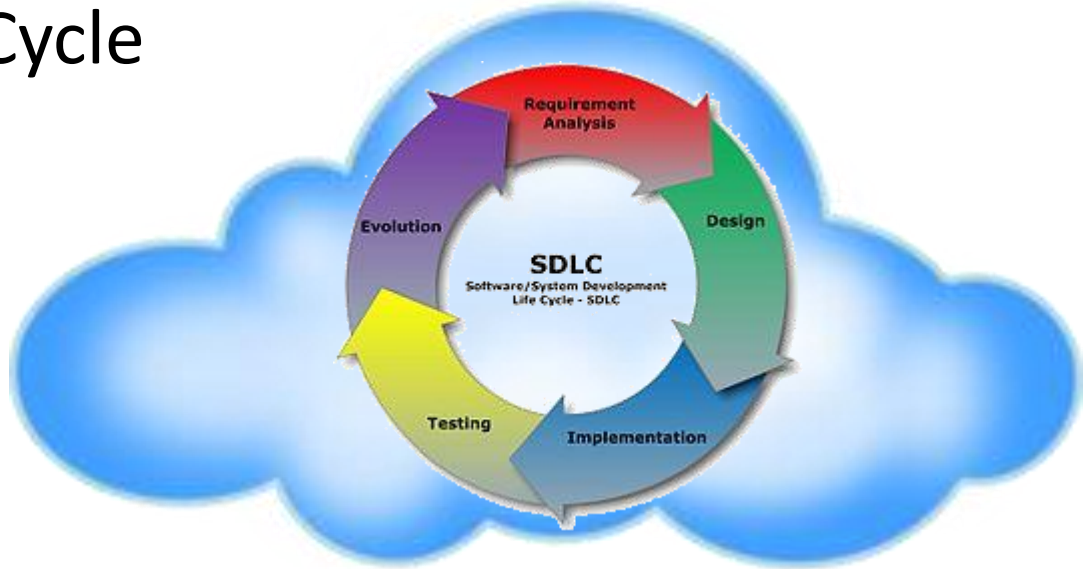
- **NoSQL DBMS as a Service**:
  - Google Datastore
  - Microsoft Azure DocumentDB
  - Amazon DynamoDB

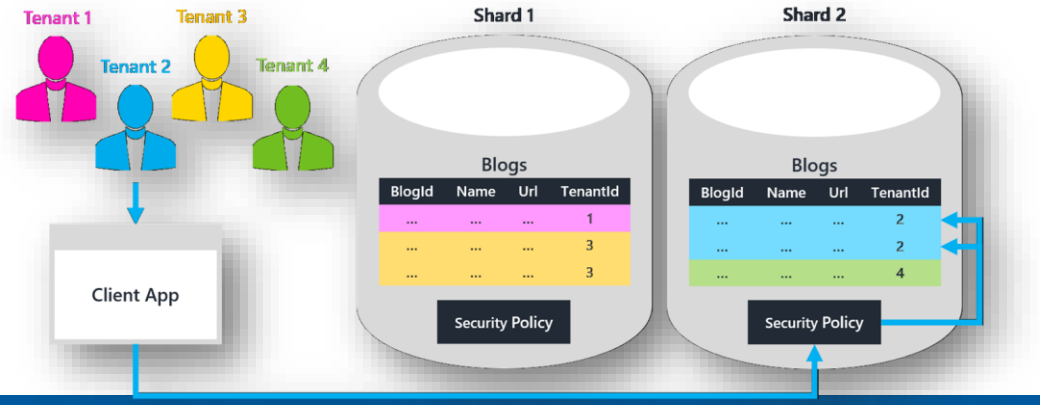
amazon DynamoDB

Platform as a Service

PaaS

- Supports the Application Life Cycle
  - Development
  - Tests
  - Deployment
- Architectures:
  - Client/Server
  - Multi-tenant





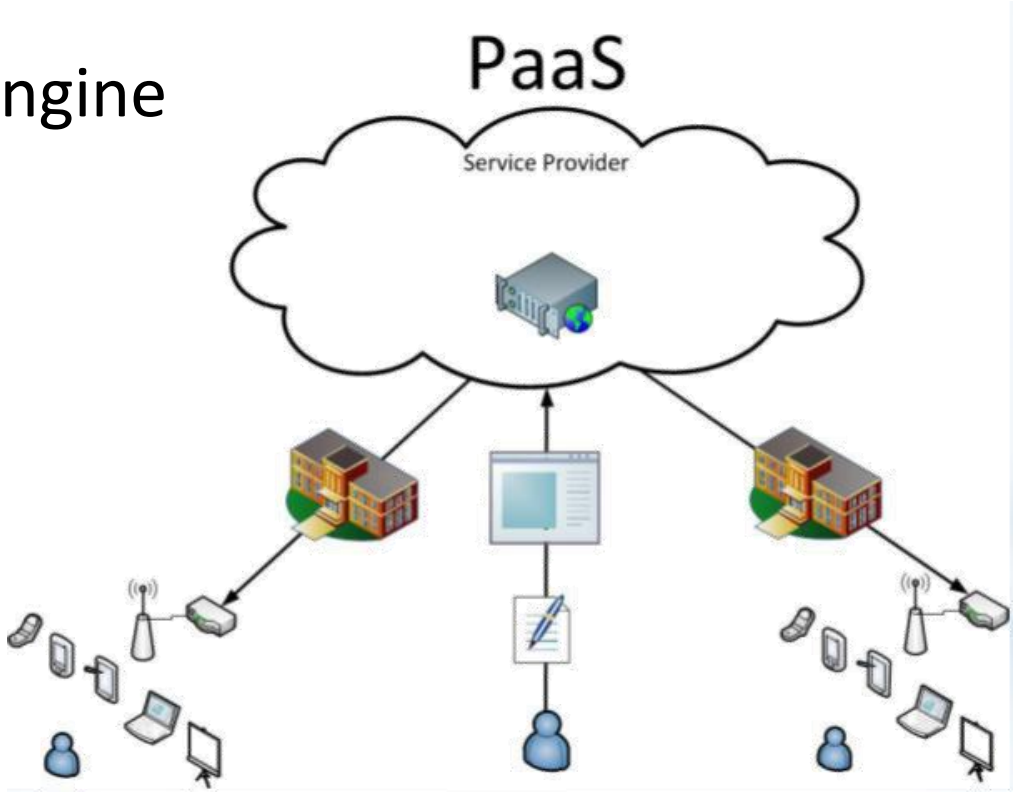
Platform as a Service

PaaS

- **Dev Mobile applications as a Service**:
  - Google App Engine / Compute Engine
  - Microsoft Azure
  - Amazon Web Services

Google App Engine Compute Engine

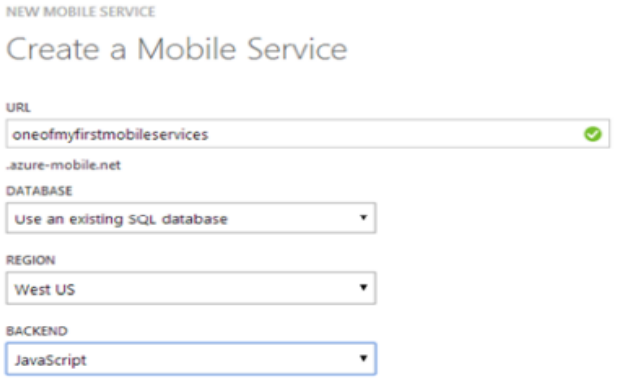
Microsoft Azure

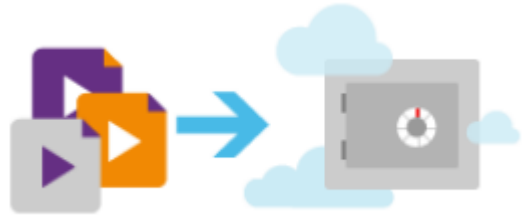


Platform as a Service

PaaS

- Develop Applications
- Build Web Sites:
  - Java, Python, .NET, …
  - Windows, Linux, Mac, Android
- Multimedia services:
  - Large scale audio and video processing & broadcas
  - Live video transmissions





Platform as a Service

PaaS

- Control Application Development

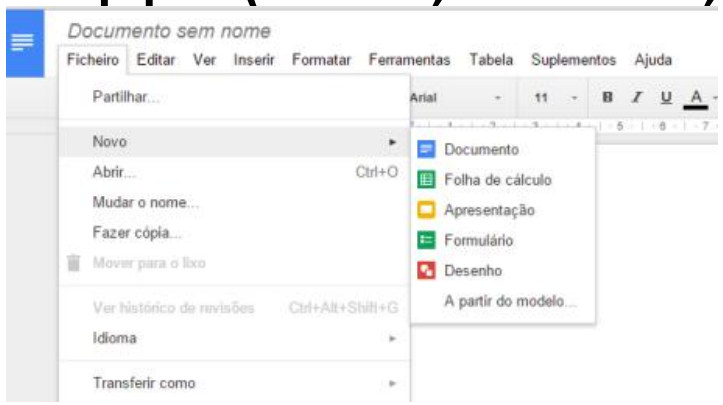
- Test Environments

- Metrics

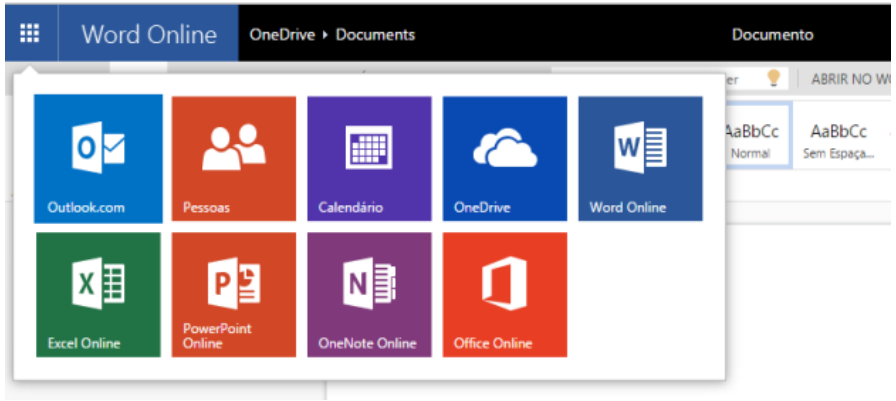
Software as a Service

SaaS

- Google Apps (Docs, Sheets, Slides)



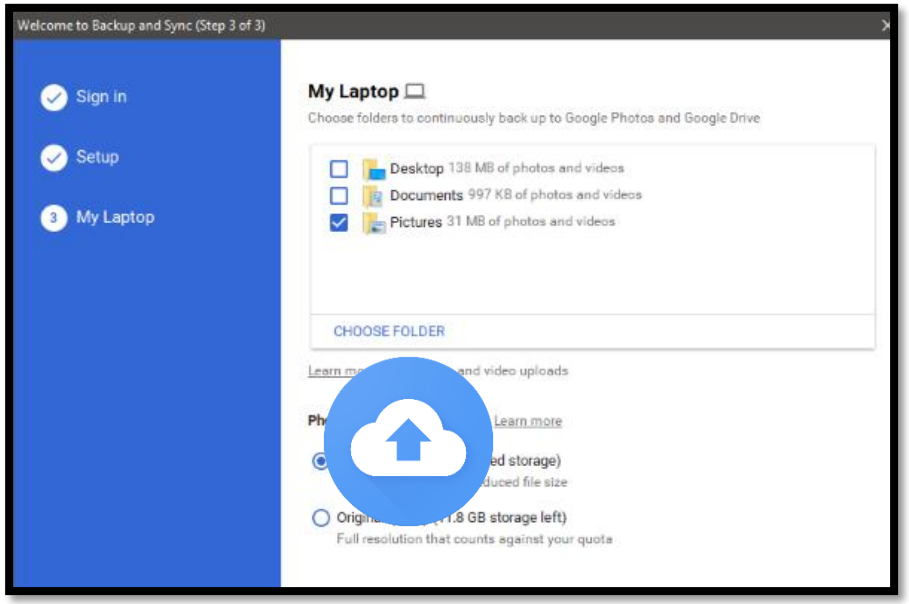
- Microsoft Web Apps (Word, Excel, Power Point)

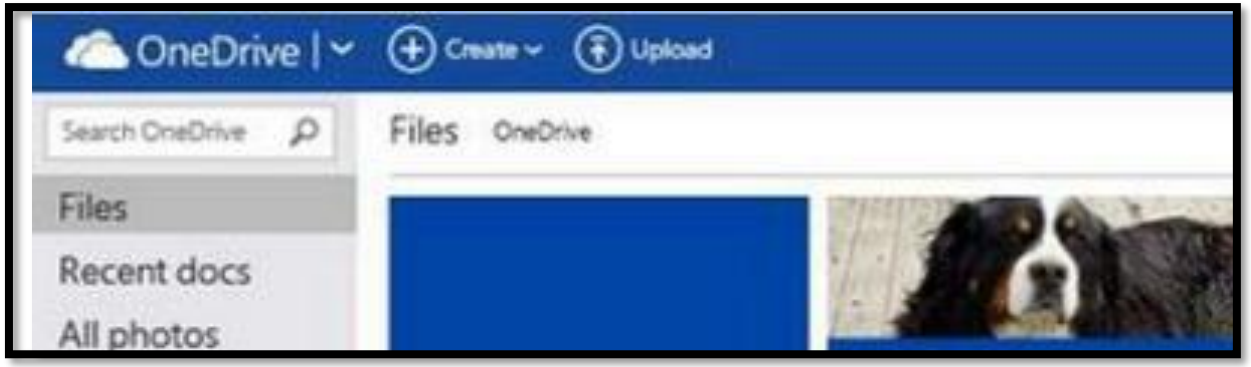


Software as a Service

SaaS

- **Storage as a Service**





Software as a Service

SaaS

- **Applications as a Service**

Mathematica

Cloud Security, Privacy & Trust

- Problem: Cloud offerings are mostly public
  - Data Encryption
  - VLAN
  - Firewalls

- Business Data Security access:
  - Public Access
  - Access Control
  - …
  - Highly Sensitive and Confidential Data

Cloud Security Threats

- All information is available at the tip of a login
  - Phishing
  - Brute force
  - DOS
  - Weak authentication systems
- Provisioning via Credit Card: Levels of IaaS
- Loss of data: Backups & Maintenance

Security – Introductory Concepts

- Objectives of a computer system
  - Data confidentiality
    - Threat: Access to information
  - Data integrity
    - Threat: Corruption of critical information
  - System availability
    - Threat: Denial of service

Security – Intruders in the system

- Potential intruders can be labelled as:
  - Occasional intruders with little technical knowledge
    - For example, users with access to shared directories that “query” other users’ files
  - Internal intruders with technical knowledge
    - They consider it a challenge and have time to “invest”
  - Individuals who want to gain advantages from the attack
    - In this category you can find:
      - personal initiative through bank account changes or blackmail
      - commercial and military espionage at the service of third parties
- Intruders of different categories have different objectives and methods

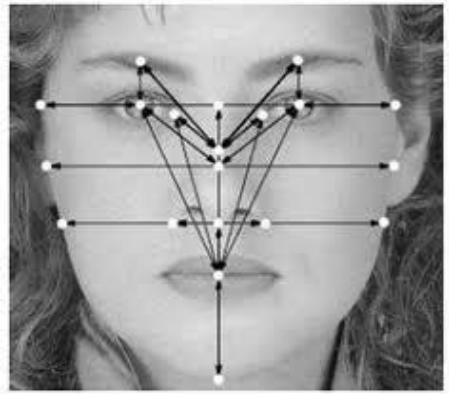
Security – Accidental Loss of Data

- In addition to threats caused by intruders, we must also consider:
  - Natural Phenomena: fires, floods, earthquakes, wars, riots, …
  - Software and hardware errors: faulty disks, program errors, …
  - Human errors: poorly entered data or commands: `rm -rf /` , …

- Ways to prevent these threats:
  - backups stored away from the originals
  - hardware redundancy (RAID, ...), etc

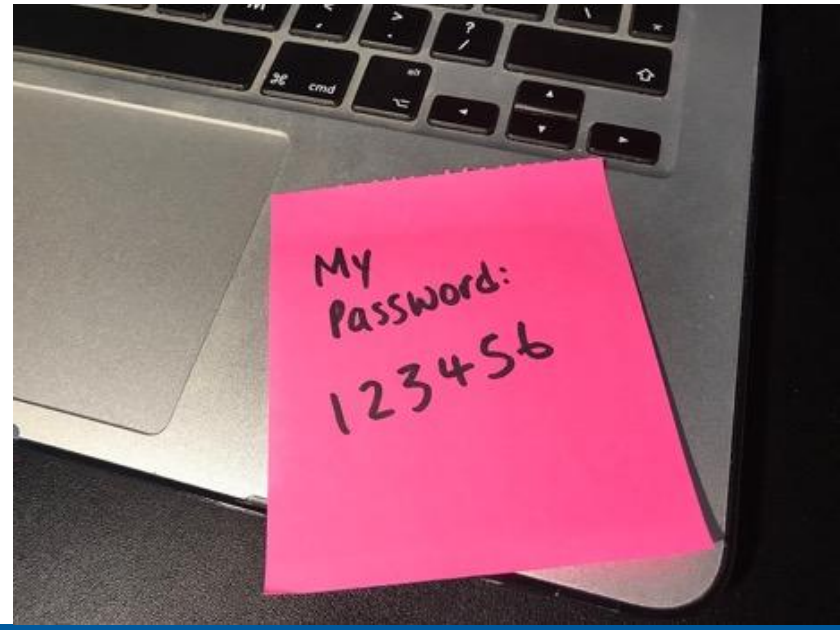
Security – User authentication

- A user who wants to log into the system must authenticate
- Authentication systems:
  - Biometrics: fingerprint, iris, photography, Face ID ...
  - Physical devices: smartcard, ...
  - Passwords
    - show asterisks, refuse invalid login, etc...
- Compromise password security...
  - Social engineering
    - Call a sysadmin, see pass under the keyboard
  - System vulnerabilities
  - Brute force attack (dictionaries, ...)



Security – Insecure passwords

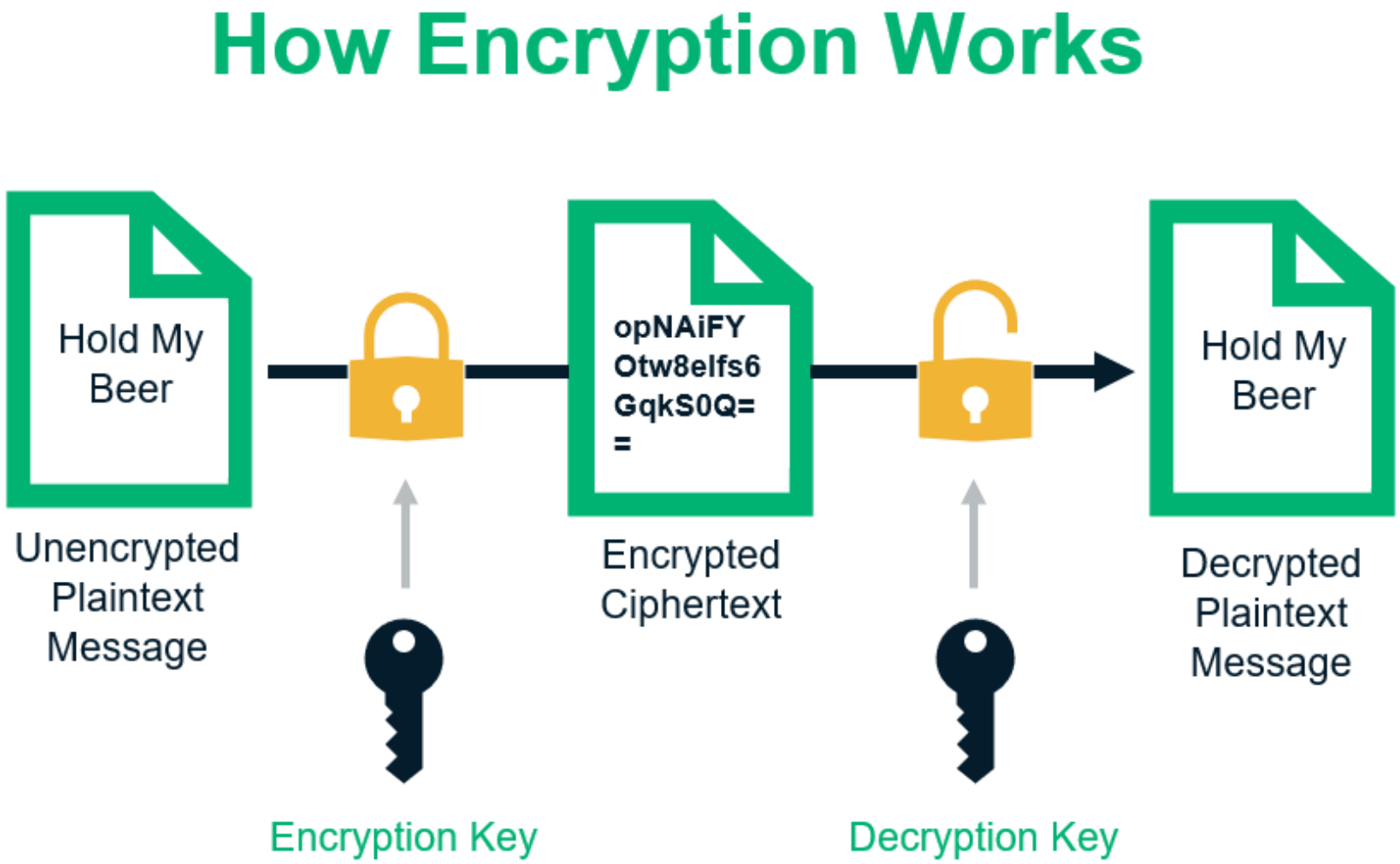
- **Top Worst Passwords of 2023**
  - https://www.zdnet.com/article/the-worst-passwords-of-2020-show-we-are-as-lazy-about-security-as-ever/
  - https://gizmodo.com/the-200-worst-passwords-of-2021-are-here-and-oh-my-god-1848073946
  - https://blog.tdstelecom.com/security/the-20-worst-passwords-of-2021/
  - https://cybernews.com/security/weakest-passwords-2022/
  - https://www.purevpn.com/blog/worst-password-list/



Security – Brute Force attacks

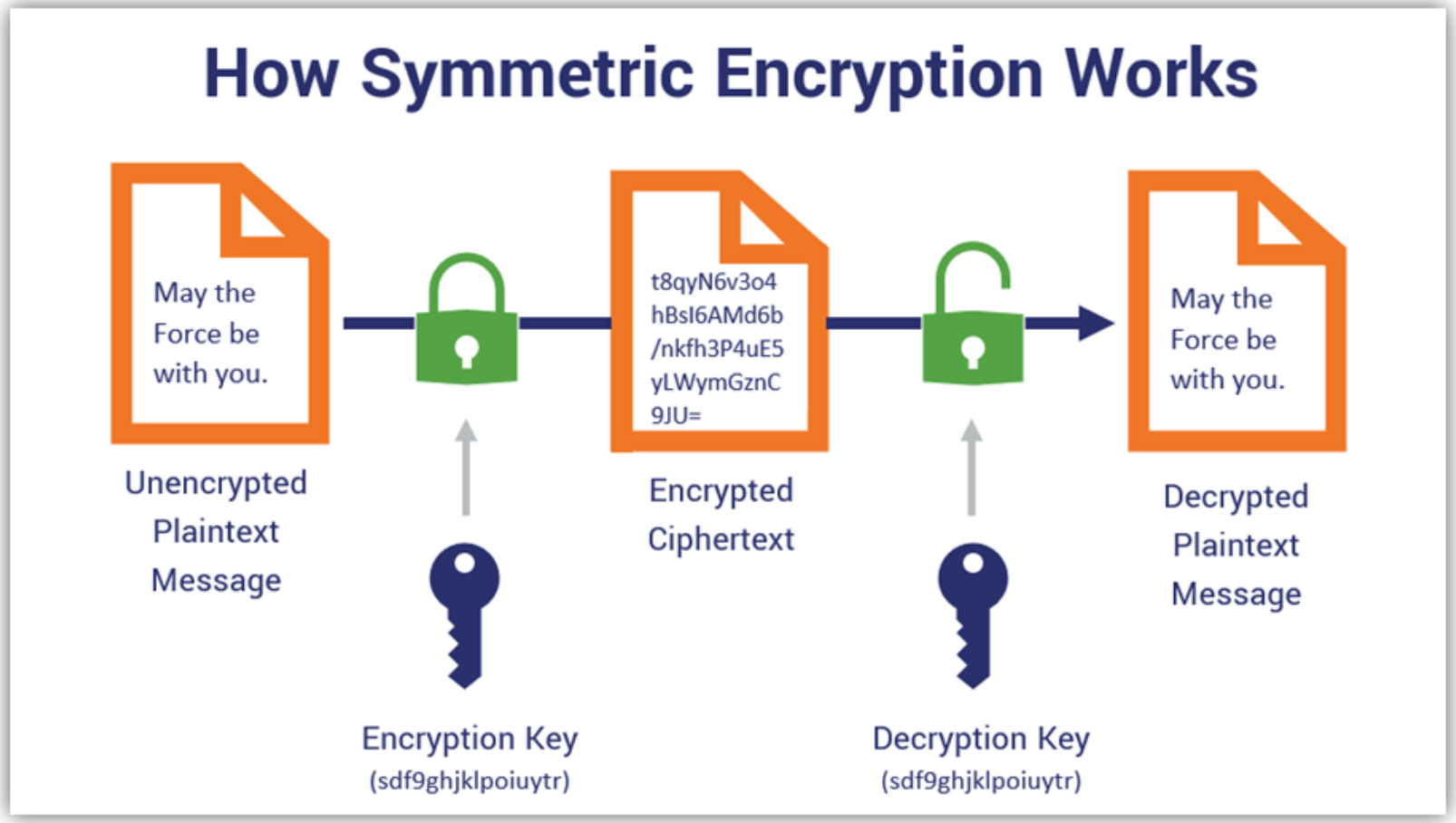
- In the old days:
  - The file `/etc/passwd` was publicly available with encrypted password
  - All it took was a dictionary and compare the passwords
- Currently, this information is encrypted in the file `/etc/shadow`
  - Harder because it can't be done offline
  - You will need to use telnet/ssh in succession
  - Automatic login/pass peer submission schemes can be tried but with great difficulty
- Challenge – answer (e.g., captcha)
  - In the creation of some web accounts, a question to avoid bots with automatic scheme

Security – Encrypting/Cyphering information



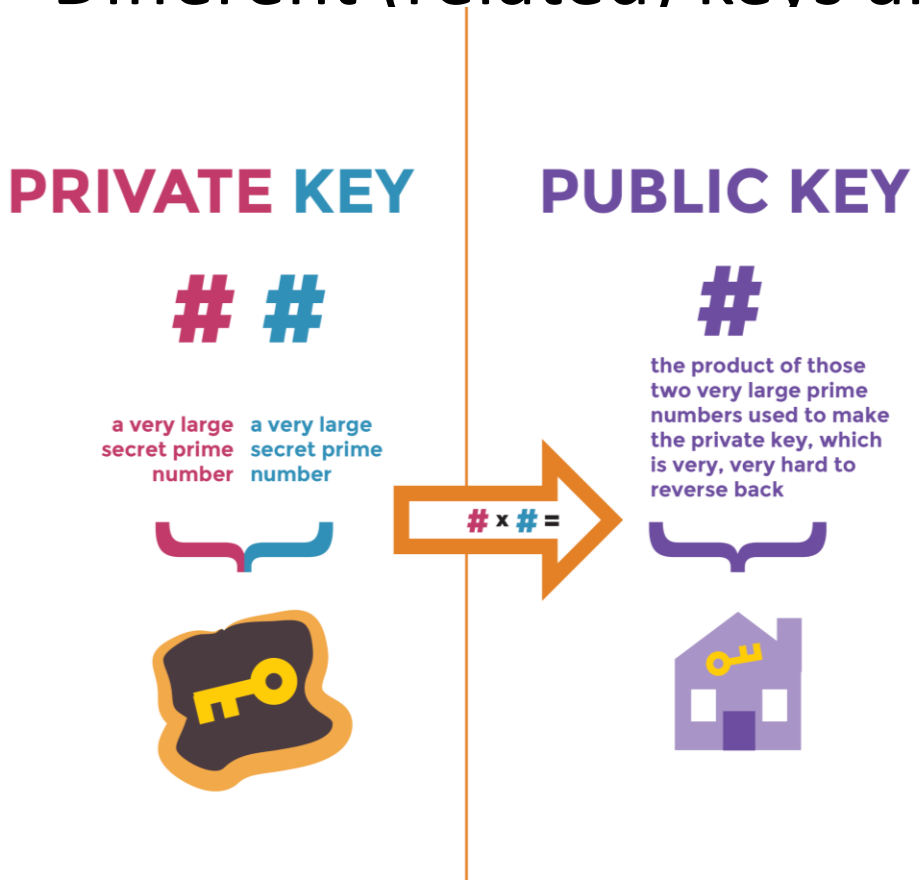
Security – Symmetric Key Pair

- The same key is used to cypher/decipher messages



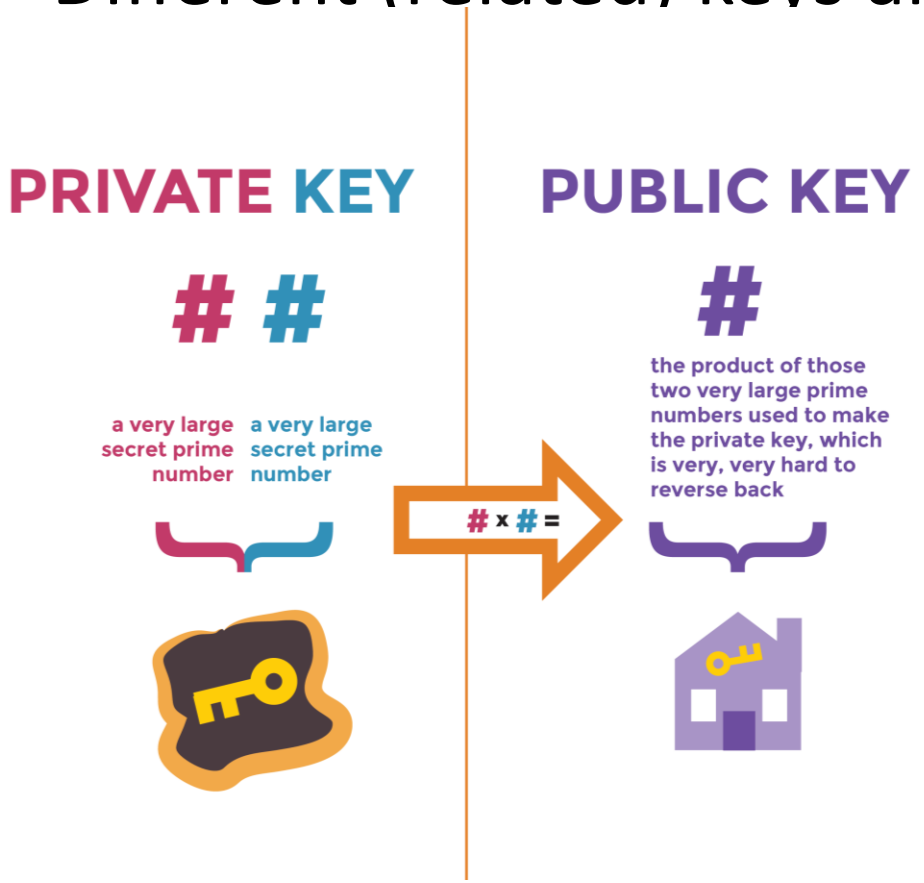
Security – Asymmetric Key Pair

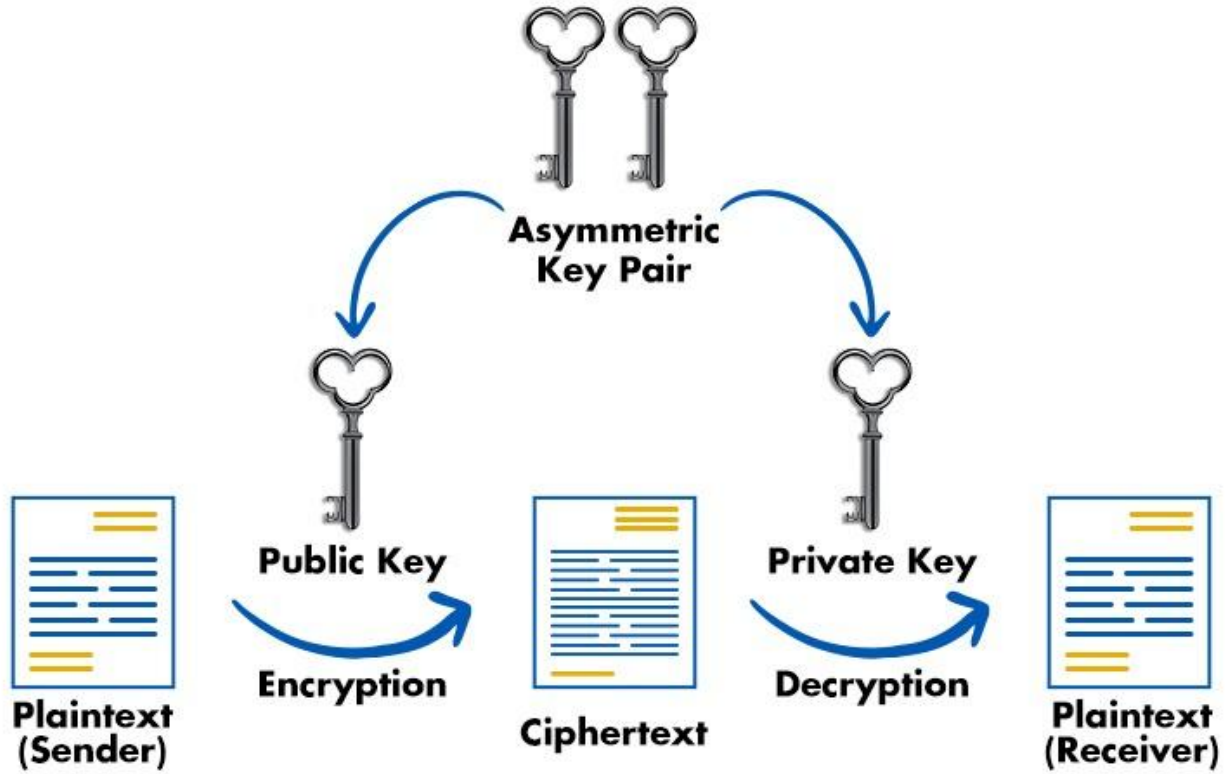
- Different (related) keys are used to cypher/decipher messages



Security – Asymmetric Key Pair

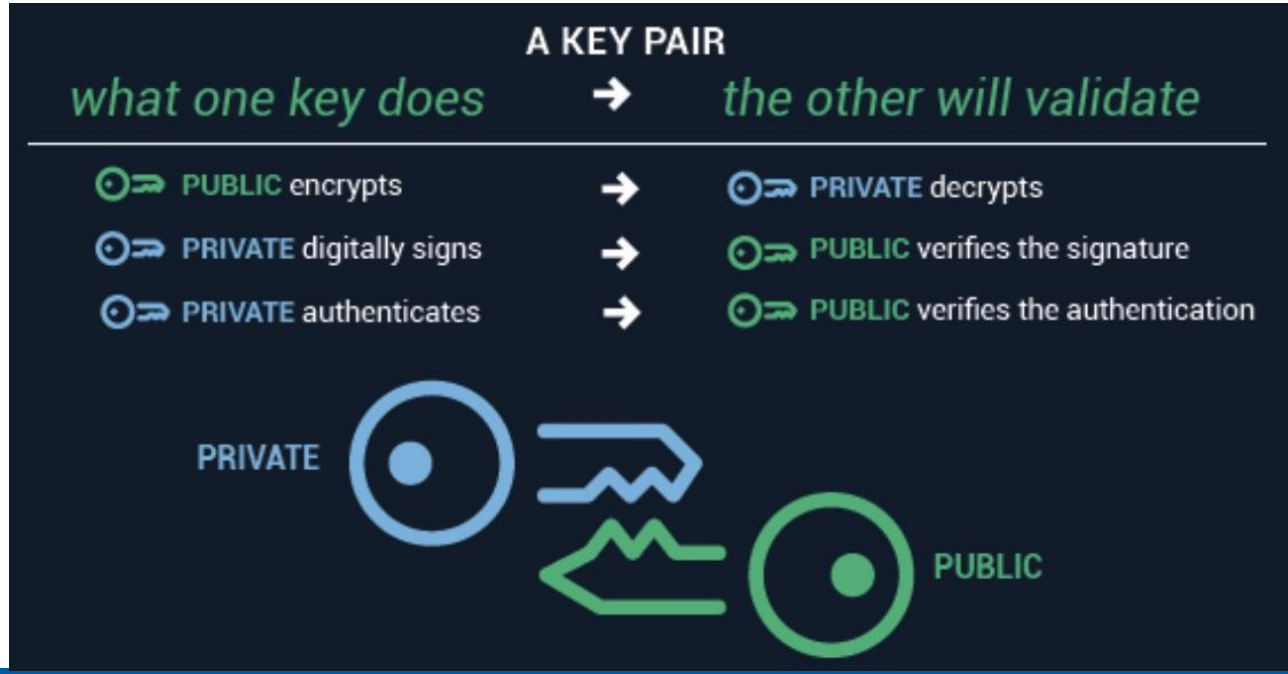
- Different (related) keys are used to cypher/decipher messages





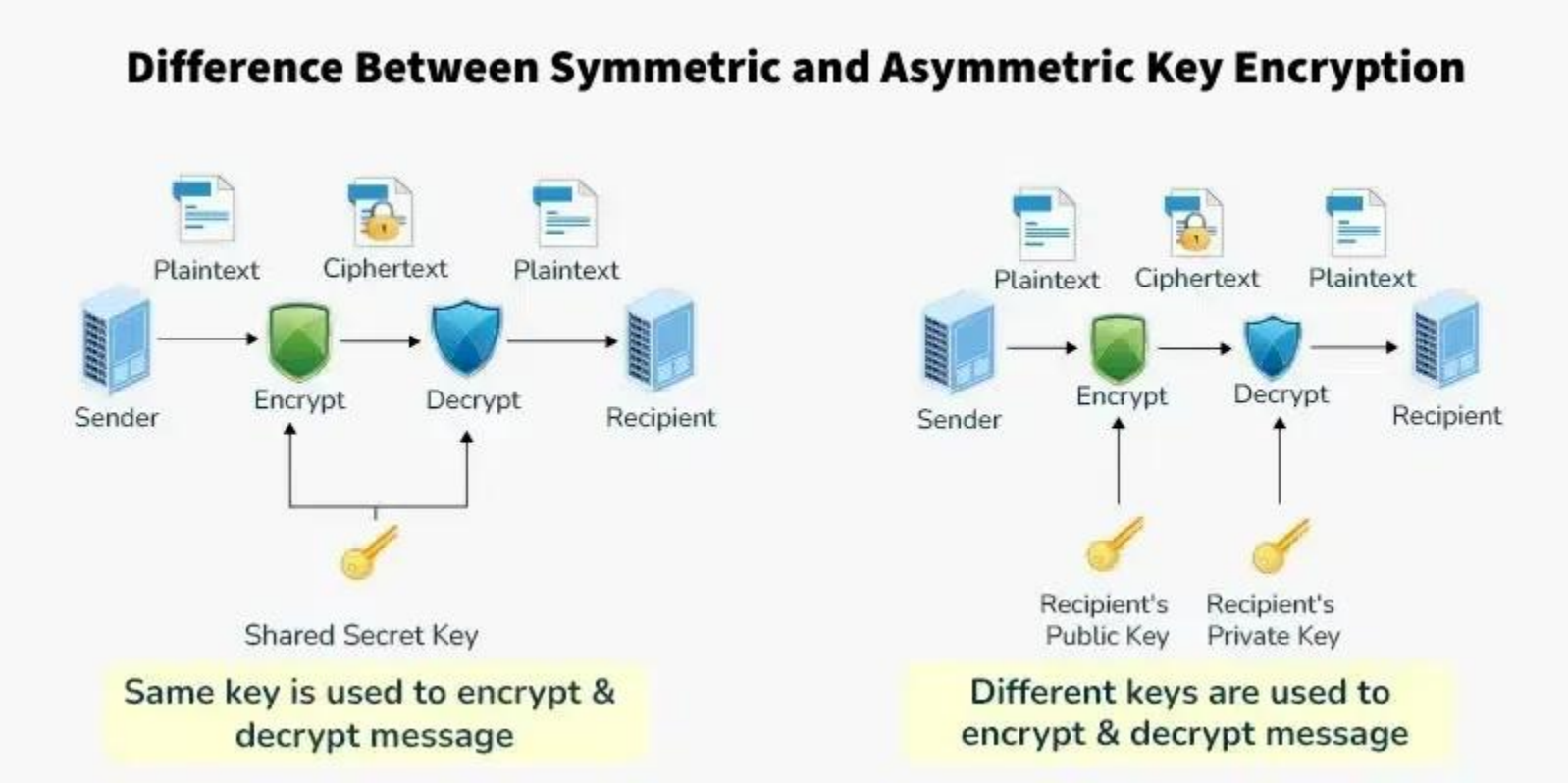
Security – Asymmetric Key Pair

- **RSA** – Well-established, stable, standard
- **Ed25519** – Modern, faster, strong with smaller key sizes
- Video – Demo
- Class – Demo:
  - Open Terminal
  - Type ssh-keygen
  - Create your key pair
  - Keys stored in folder **`~/.ssh/`**



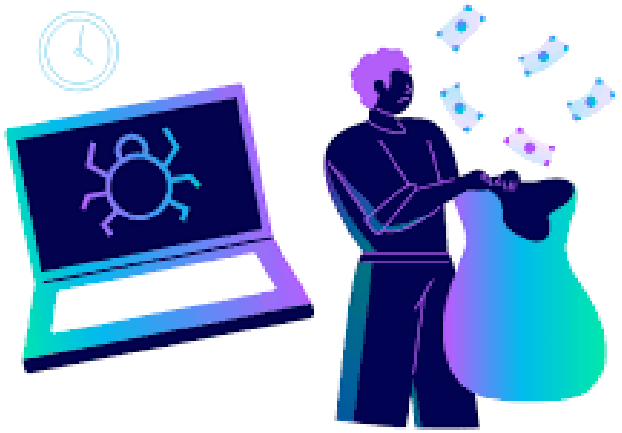
Security – Key Pair

- Symmetric Key Pair
- Asymmetric Key Pair



Security – Attacks from within the system

- Attacks performed after the user has logged in
- Goals
  - Get a higher degree of system permissions
  - Get accounts on other machines

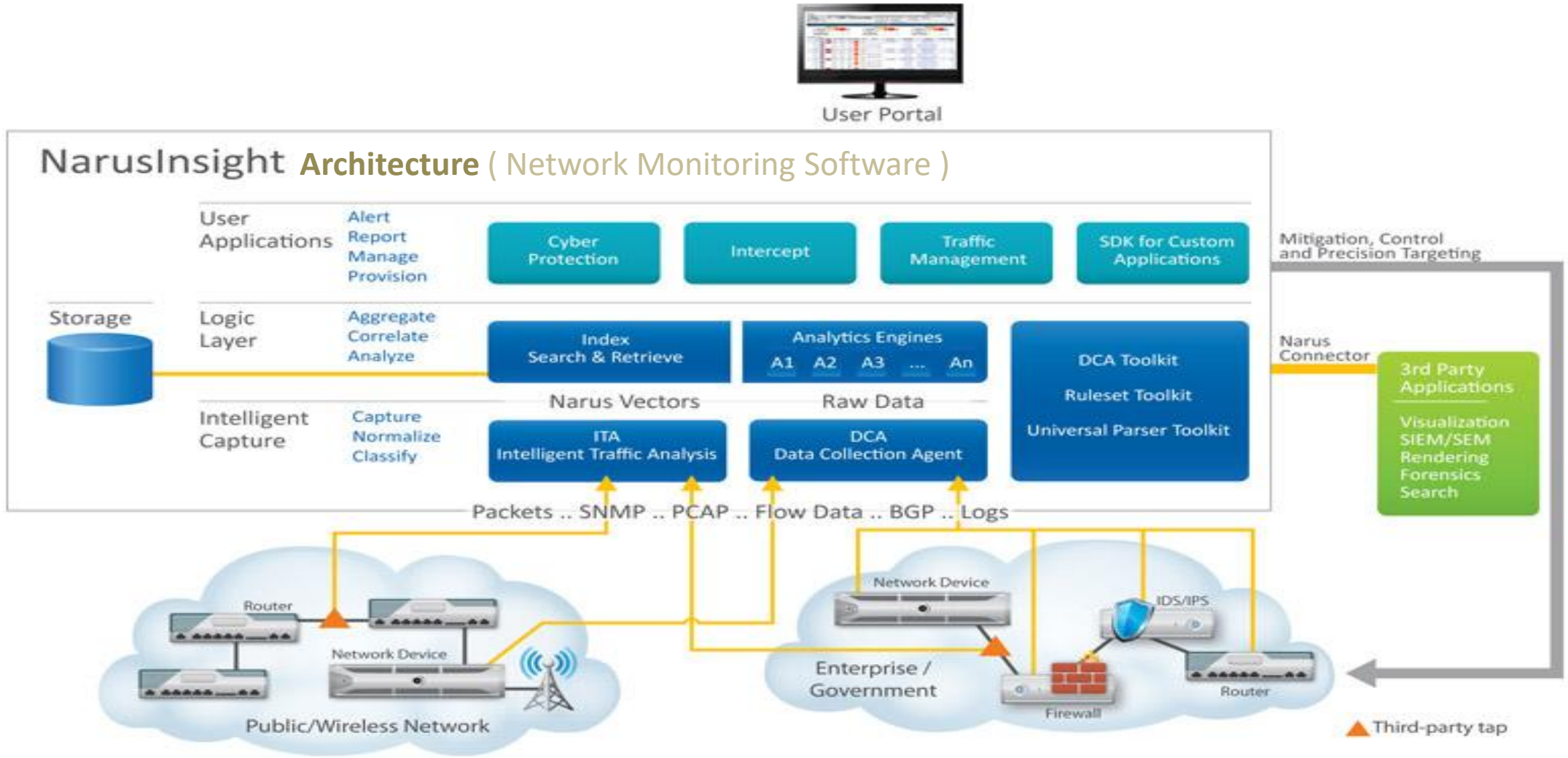


Security – Attacks from within the system

- Some techniques:
  - Trojan - Application that replaces the original
    - You have to be root or take advantage of PATH issues
    - Example: ftp, login, ... with different behavior
      Program that replaces "login" and sends your pass via email
    - There are root kits with Trojans already prepared for different systems

  - Sniffing - Application listening to network card traffic (intercepting connections to other machines) or even from any network (HUBs, broadcast on switches)
    - capsa free - Portable network analyser (packet sniffer) freeware for windows
    - Carnivore, later renamed DCS1000, was a system implemented by the FBI
    - Wireless Diagnostics – “secret” packet Sniffer in OS X
    - dSniff, sniffit, tcpdump, wireshark ...

Security – Attacks from within the system



Security – Attacks from within the system

- Some techniques:
  - Spoofing – Assumes impersonating those who are not
    - Server spoofing: IP hijacking
    - Login spoofing: make a program that looks like the system program which asks for login and pass.
    - Spoofing of MAC Address
  - Logical bombs – a program that, if a certain operation is not performed regularly, such as entering a password, triggers an illicit action on the system. Potentially used by employees for fear of layoffs

Security – Attacks from within the system

- Some techniques:
  - Trap doors – code entered by system programmers to bypass identity checks
    - For example: if "xpto" is entered as user, a system does not ask for a pass
  - Buffer overflow – derived from many systems written in C. The C compiler does not check writing outside the boundaries of an array
    - Example:

```
char phrase[100];
phrase[1024]=0;
```

      - We can then overwrite the Return Address of the function with illicit code.
        Using the gets() function is a source of these attacks. Therefore, the compiler warns for it
        More serious in programs that run with root privileges

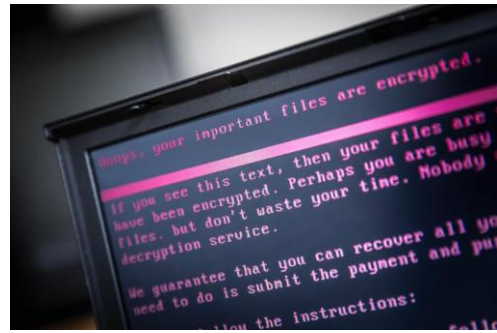
Security – Attacks from within the system

- Other techniques (remote attacks):
  - Internet Worms – viruses that spreads between machines of the same network, using an existing vulnerability

- Terminology:
  - Exploits (programs that exploit vulnerabilities in the system or their applications) mostly taking advantage of Buffer Overflows
  - "Script Kiddies" are people who don't realize they are performing attacks they perform as they only follow "recipes". These are generally available in websites or on IRC channels

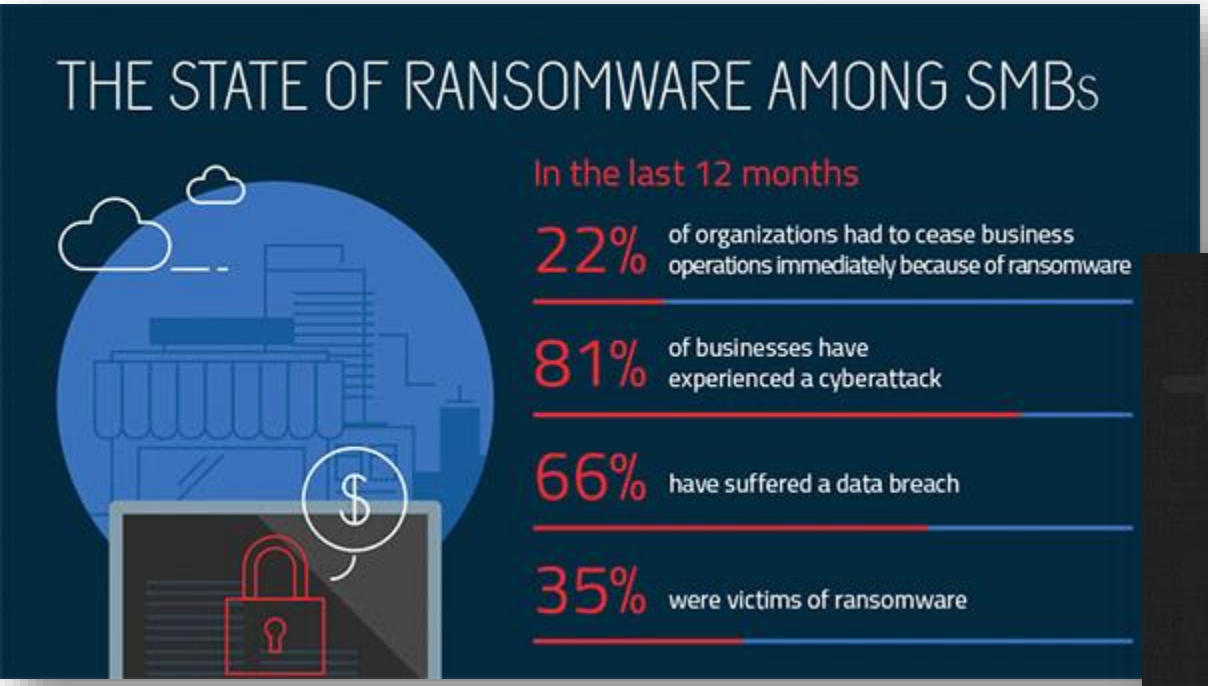
Ransomware

- Cyphers the Hard Disk and requests a ransom for decoding it
- Starting in 2017:
  - WannaCry
  - NotPetya → It led Maersk (Logistics and Transport) to lose revenues of more than 300M$
- The attacks peaked in 2019
- Attacks on government agencies and SMEs

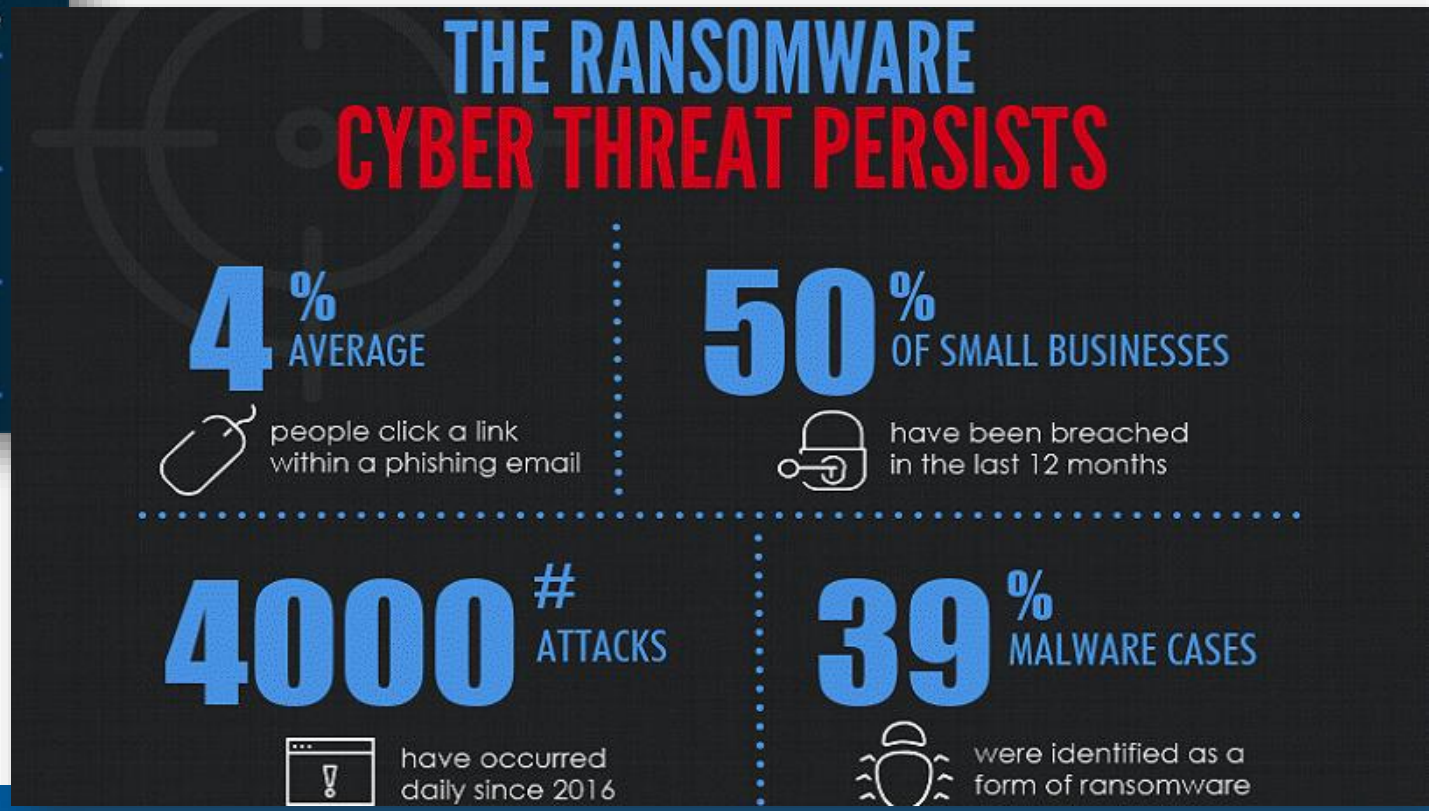


- SamSam Ramsomware – The Government of Atlanta paid $2.6M to solve the problem (but the Hackers only asked for $52K)

Ransomware in Small and Medium Businesses

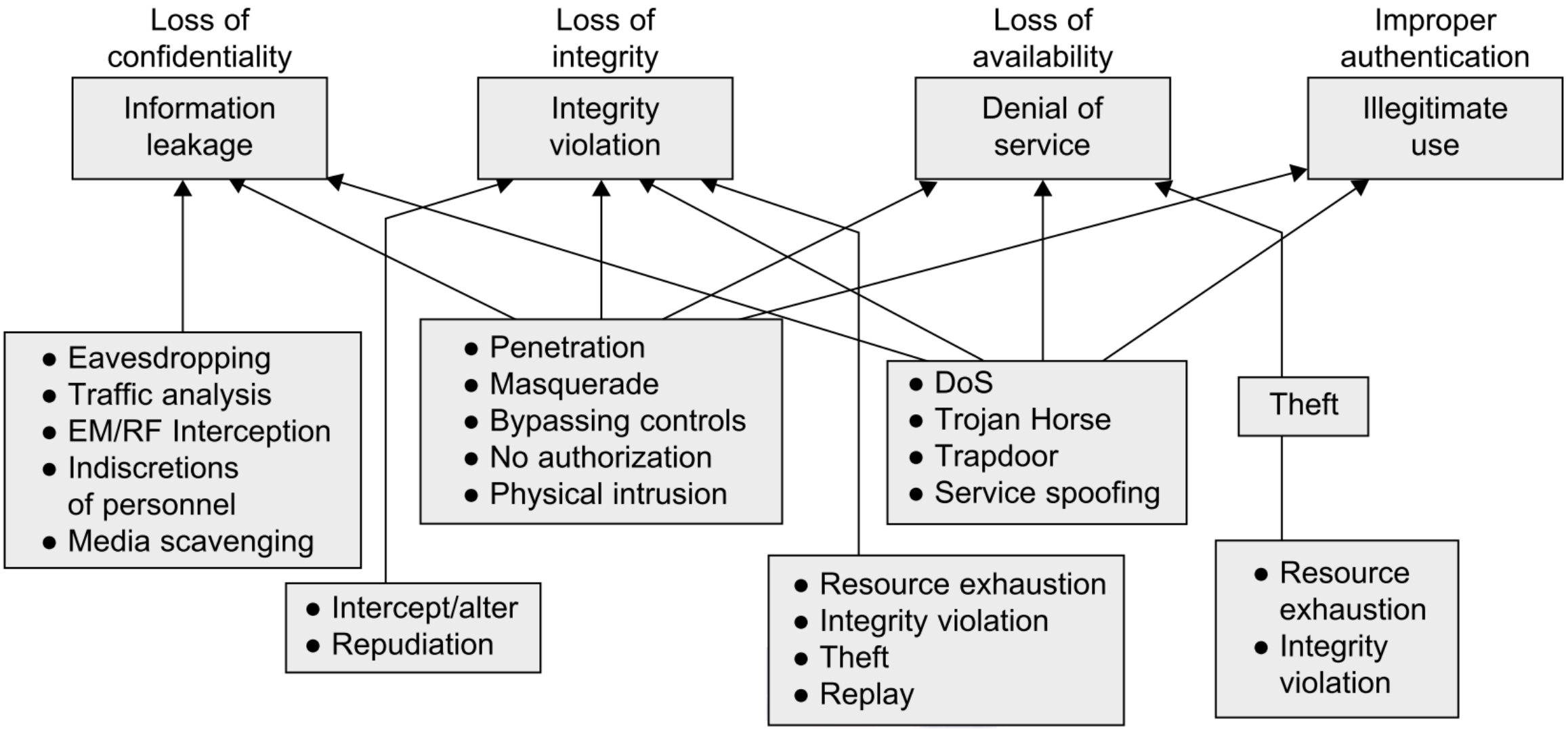


At the end of 2017 it calmed down:
People make more backups, etc.



In 2018, the hackers became smarter.
The ransomware first destroys backups before it becomes visible

Security Vulnerabilities



Deep Web

- Deep Web
  - aka Deepnet, invisible Web, DarkNet, Undernet, Dark Web …
  - World Wide Web content that is not part of the Surface Web.
    Not indexed by standard search engines.
- Darknet
    - network that can only be accessed with specific software, configurations, or authorization
- Tor Browser (https://www.torproject.org)
    - protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked

Security – How to protect from attacks

- Firewalls, DMZs and rule definition
- Secure Communications (SSH)
- Policy making
- Vulnerability auditor (Nessus, Saint, OpenVAS, ...)
- Intrusion Detection System's (Snort, Narus)
- Digital file signature (tripwire)
- Interpretation of logs (scanlogd)
- ...

Cybersecurity

- https://www.youtube.com/watch?v=inWWhr5tnEA
- https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

- Potential risks:
  - Malware (Virus, Trojan, Adware, Spyware)
  - Phishing (identity theft)
  - Ransomware
  - Man-in-the-middle (ex: eavesdropping)
  - Weak passwords
  - SQL Injection
  - DDoS
  - Adware

- Mitigation:
  - Firewalls
  - "Honey pots“
  - Antivirus
  - Strong passwords
  - Multi-factor authentication

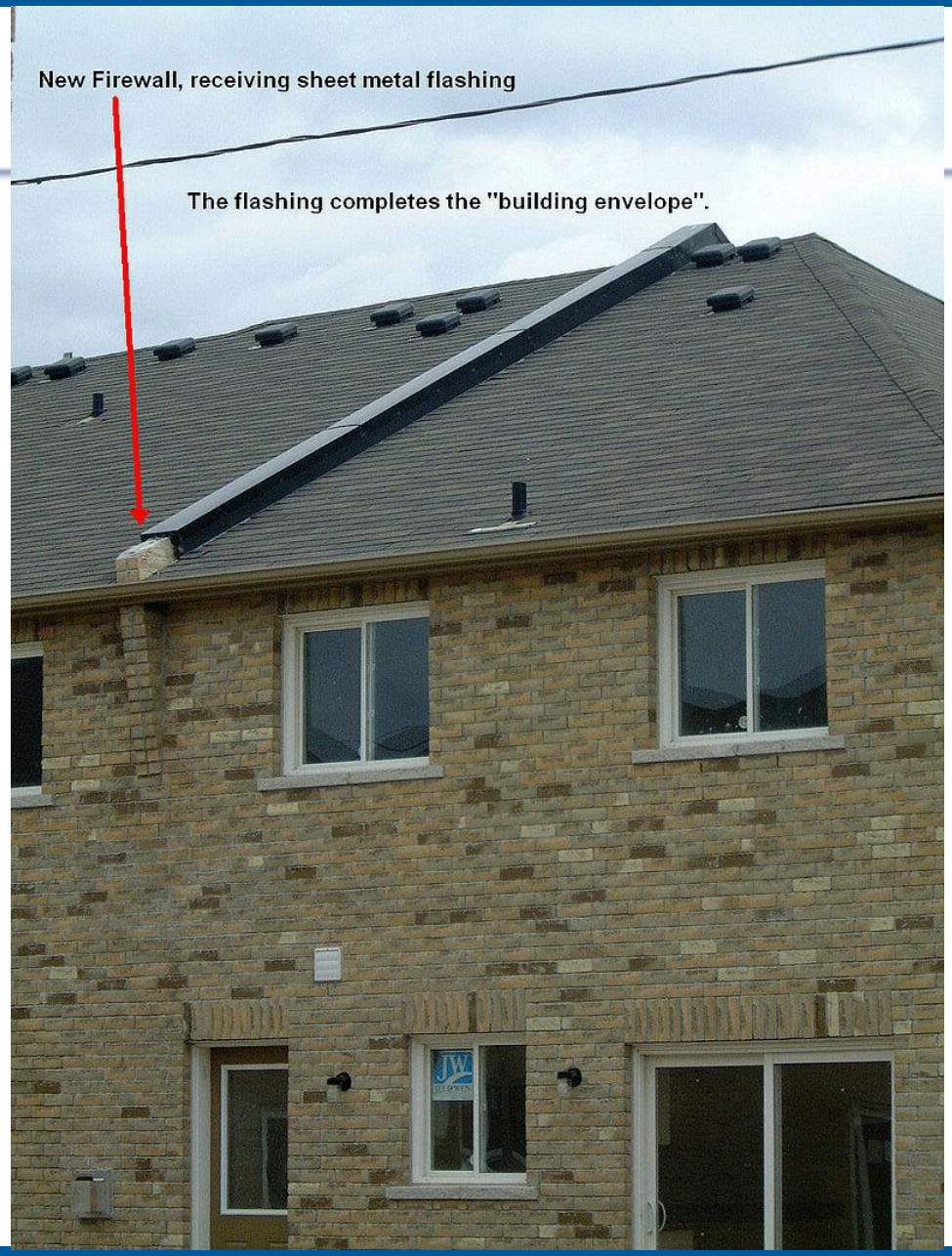
Cybersecurity

- The national entity that governs Cybersecurity in Portugal is the National Cybersecurity Center (CNCS)
  - Quadro Nacional de Referência para a Cibersegurança (QNRCS)
  - https://www.nau.edu.pt/curso/consumidor-ciberseguro/
  - https://www.nau.edu.pt/curso/cidadao-ciberinformado/
  - https://www.cncs.gov.pt/recursos/webcheckpt/

Cybersecurity: Types of Security

- **Application security:**
  - Vulnerability analysis and correction
- **Network Security:**
  - Antivirus, Firewalls
- **Operational security:**
  - Identification of critical information
  - Risk management about this information
- **Disaster Recovery:**
  - Disaster Recovery Plans, Business Continuity Plan

Firewall

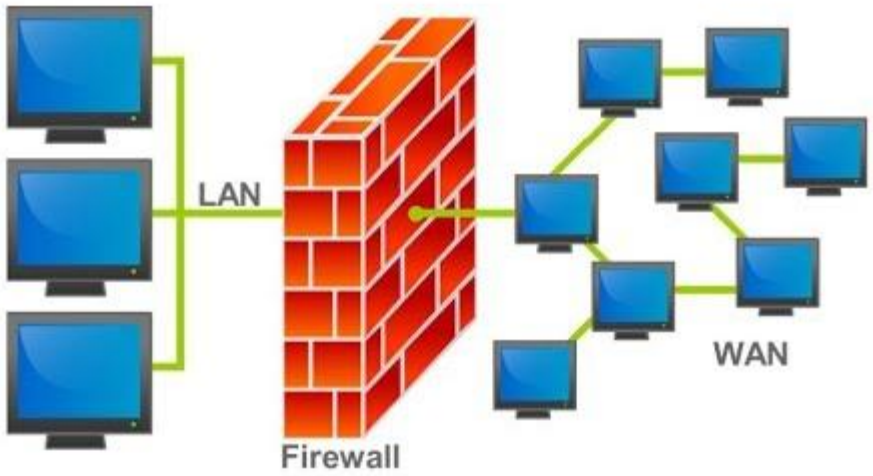


containment wall

Firewall

- A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules

- Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet



https://www.youtube.com/watch?v=kDEX1HXybrU

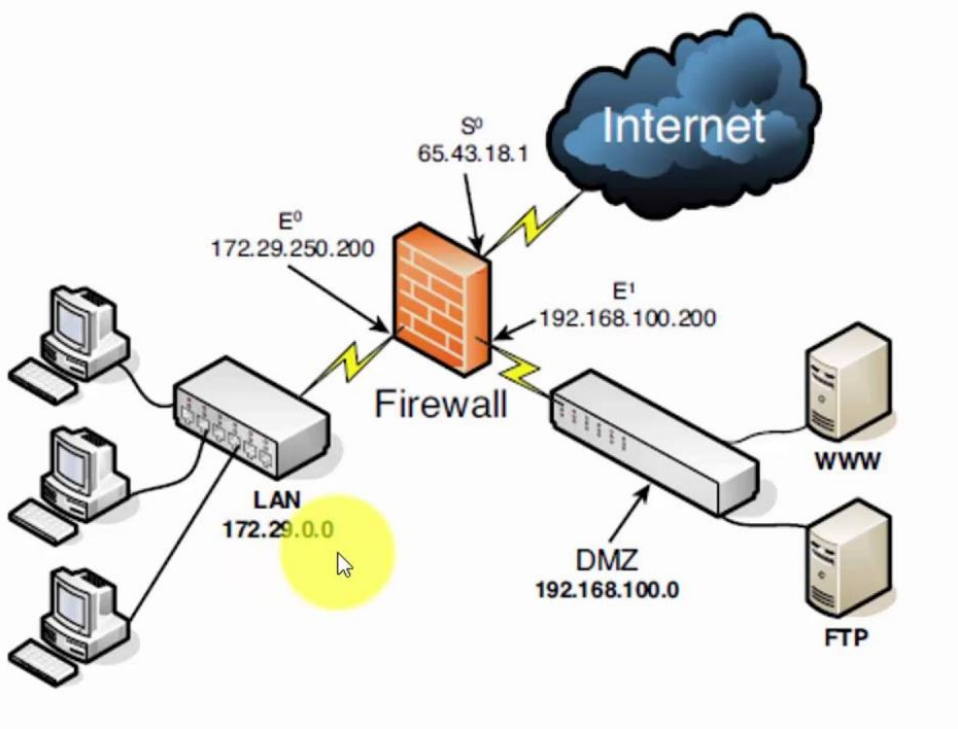
https://www.youtube.com/watch?v=5geL5yHpa2Q&feature=emb_logo

Firewall

- A **firewall** is a system designed to **prevent unauthorized access** to or from a private network
- Firewalls **prevent** unauthorized internet users from **accessing** private networks connected to the internet, especially **intranets**
- **All messages** entering or leaving the intranet (the local network to which you are connected) **must pass through the firewall**, which examines each message and blocks those that do not meet the specified security criteria
- You can **implement** a firewall in either **hardware (appliance)** or **software** form, or a combination of both
- In protecting private information, a **firewall** is considered a **first line of defense**; it cannot, however, be considered the only line
- **Firewalls** are generally designed to protect network traffic and connections, and therefore **do not attempt to authenticate** individual users when determining who can access a particular computer or network

DMZ: Demilitarized Zone

- https://www.youtube.com/watch?v=dqlzQXo1wqo
- https://pplware.sapo.pt/truques-dicas/o-que-o-seu-router-e-capaz-de-fazer-v/

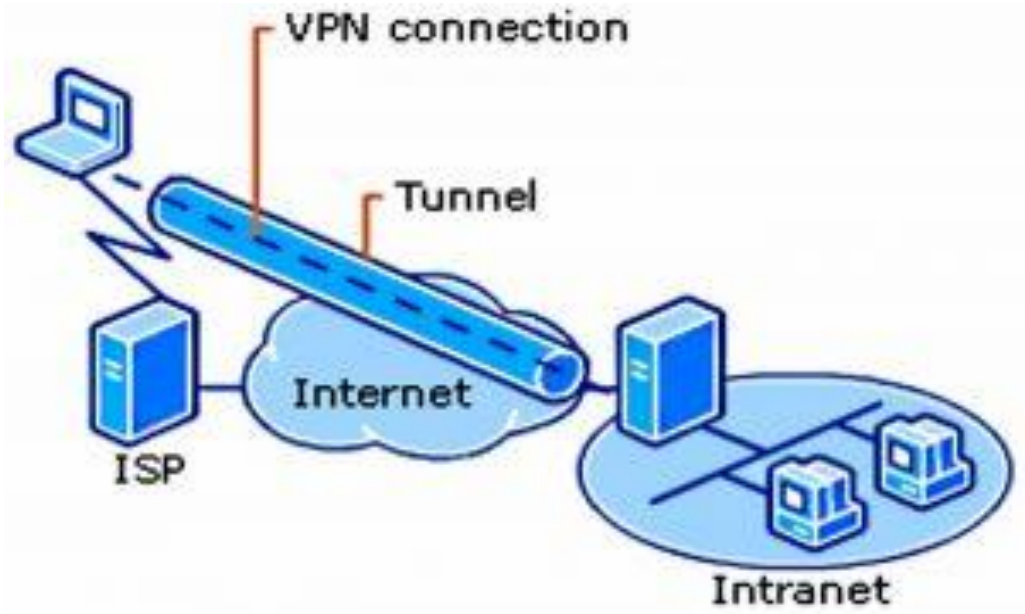


VPN: Virtual Private Network

- https://www.youtube.com/watch?v=X-z07FSlji4&feature=emb_logo
- https://www.youtube.com/watch?v=gX1nM_p0m0I
- https://www.youtube.com/watch?v=xGjGQ24cXAY

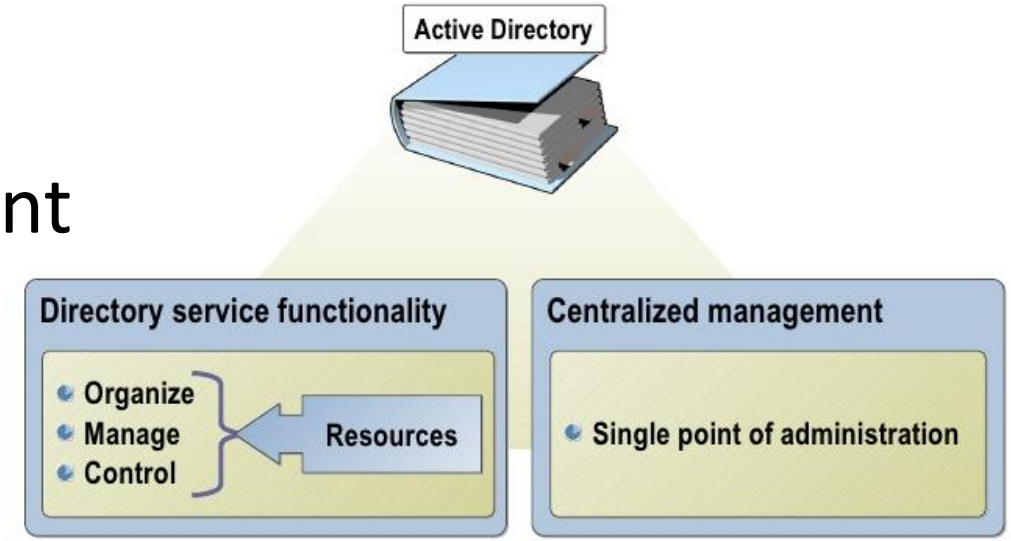
OPENVPN

- Secure channel to make a machine "invisible" on the internet



Active Directory

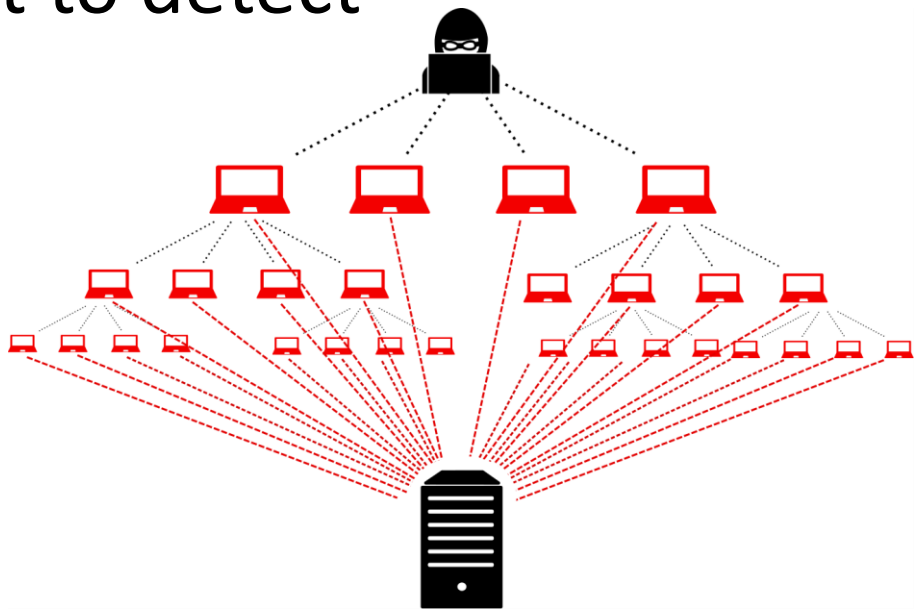
- https://www.youtube.com/watch?v=GfqsFtmJQg0
- Program typically installed on Servers
- Centralized authentication management
- List of Users and Groups
- Target → Authentication Security Management



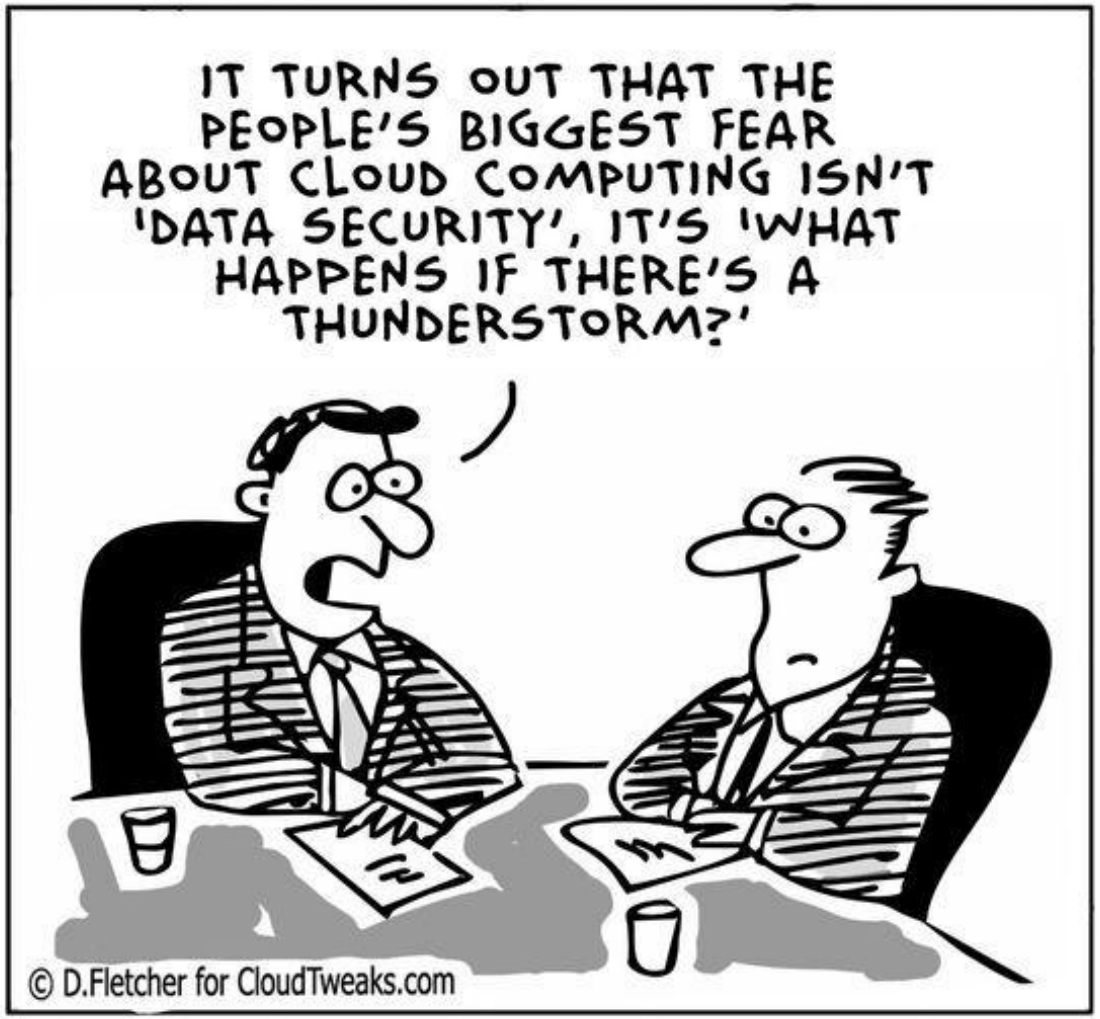
DDoS: Distributed Denial of Service

- https://www.youtube.com/watch?v=ilhGh9CEIwM

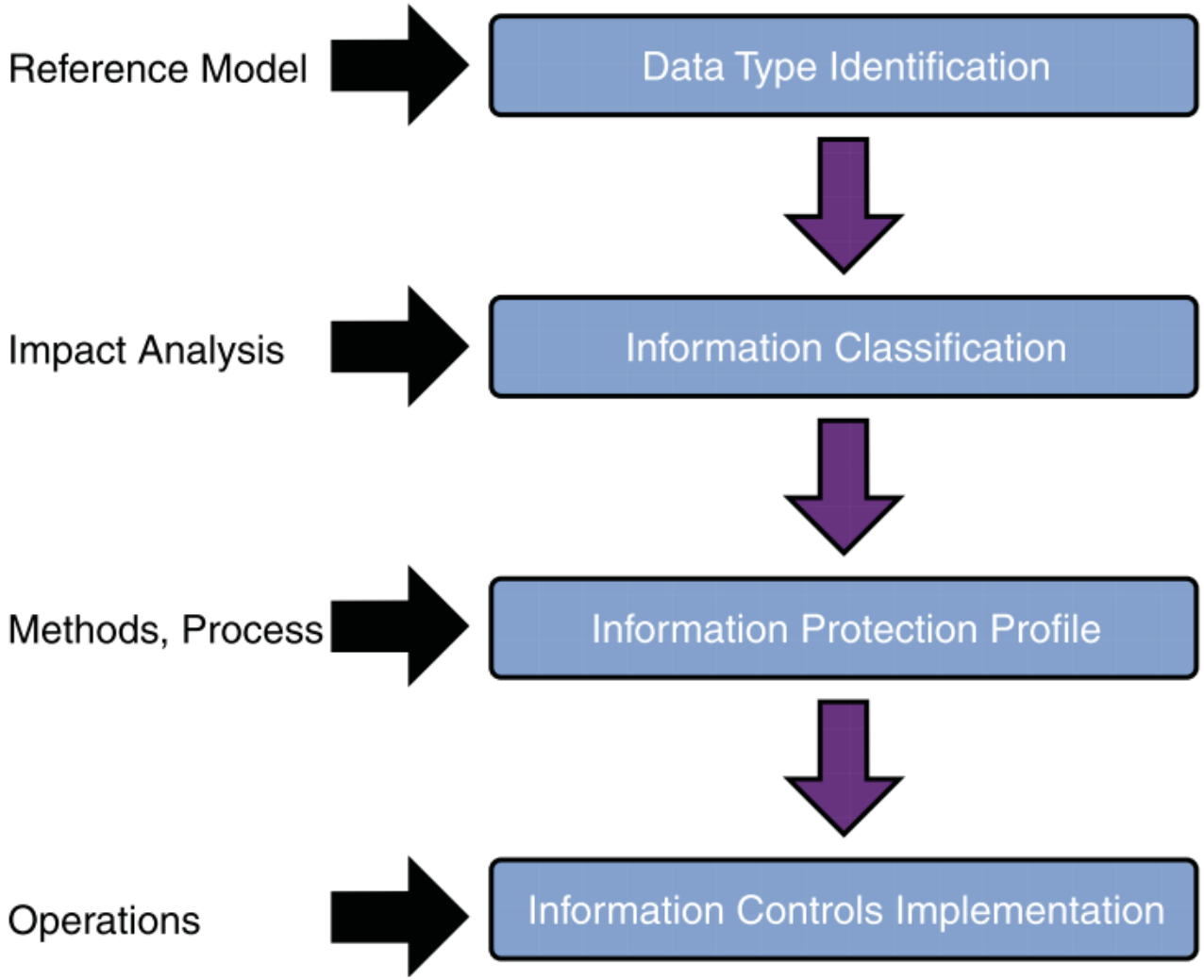
- DoS is already a problem
- being distributed is much more difficult to detect
- Uses botnets



Cloud Security



Cloud Security Profiling Model



Business Impact Levels (BIL)

- **BIL6, Top Secret (TS):** The highest level of classification of material on a national level. Such material would cause “exceptionally grave damage” to national security if made publicly available.
- **BIL5, Secret:** Such material would cause “grave damage” to national security if it were publicly available.
- **BIL4, Confidential:** Such material would cause “damage” or be “prejudicial” to national security if made publicly available.
- **BIL3, Restricted:** Such material would cause “undesirable effects” if made publicly available. Some countries do not have such a classification.
- **BIL2, Protect:** Information or material that if compromised, would likely cause substantial distress to individuals or, for example, breach statutory restrictions on the disclosure of information.
- **BIL1, Protect:** Technically not a classification level, but is used for government documents that do not have a classification listed previously. Such documents can sometimes be viewed by those without security clearance.
- **BIL0, Unclassified:** Information that is available to the general public and would not cause any harm or infringe any law were it to be intentionally or accidentally disclosed to the general public.

Risk Analysis

- **Penetration testing:** Penetration testing tests for the depth of vulnerabilities in specific applications, hosts, or systems. This type of testing poses the greatest risk to the resource and should be used sparingly.

- **Vulnerability Analysis (VA):** A vulnerability analysis considers the breadth of scope and might include testing methods ranging from simple network scanning using automated or manual tools to complex testing through automated electronic means.

- **Risk Assessment Model (RAM):** A RAM combines the standard ISO requirements with an enterprise's information security requirements using various frameworks (standardized or in-house). This tends to lead to a process that is organization unique, having its own scoring model to identify strengths and weaknesses in the overall information security posture.

Cisco Criticality SLA Table

C-Level	Term	Impact Description
C1	Mission Imperative	Any outage results in the immediate cessation of a primary function,* equivalent to the immediate and critical impact to revenue generation, brand name, and/or customer satisfaction; no downtime is acceptable under any circumstances.
C2	Mission Critical	Any outage results in the immediate cessation of a primary function, equivalent to a major impact to revenue generation, brand name, and/or customer satisfaction.
C3	Business Critical	Any outage results in the cessation over time or an immediate reduction of a primary function, equivalent to a minor impact to revenue generation, brand name, and/or customer satisfaction.
C4	Business Operational	A sustained outage** results in the immediate cessation of a primary function.
C5	Business Administrative	A sustained outage has little or no impact on a primary function.

Cloud Risks

- Regional Compliance
  - Providers: geographically dispersed data centres
  - Legal problems
  - Different legal access to data:
    - USA PATRIOT Act (2001)
    - European Union Data Privacy Directive (1995)
    - Canada
    - Australia
    - …

Cloud Management Difficulties

- Service Oriented approach:
  - Appropriate and formal design of Services and APIs
  - Flexible approach for deploying/accessing services
  - Holistic perspective on integration of the services

- Synchronisation of Local/Private/Public Data:
  - Clear definition of access policies
  - Synchronise Local Data and Cloud Remote Data
  - Distribution of data among all storage siloes
  - Redundancy and error handling

Cloud Management Difficulties

- Security Policies definitions:
  - Management of Services Inside & Outside Firewalls
  - Integrated service delivery

- Management of Configurations and Licences
  - Heterogeneous set of environments
  - Different types of requirements
  - Different Handling of each environment
  - Coordination of management activities

Cloud Management Difficulties

- Management of SLAs:
  - Different cloud providers with different SLAs
  - Public, Private, Hybrid and Local services' SLAs
  - Different Customer SLAs per service

- Support of Security and Governance:
  - Development of Security strict Policies and Rules
  - Development of Governance Guidelines and Rules
  - IT and Business integrity
  - Adding new providers

Cloud Management Difficulties

- Elasticity:
  - Most architectures are not designed for elasticity
  - Elastic architectures require:
    - Real-time application workload monitoring
    - Scalable application components
    - Real-time automation of resource provisioning and disposal

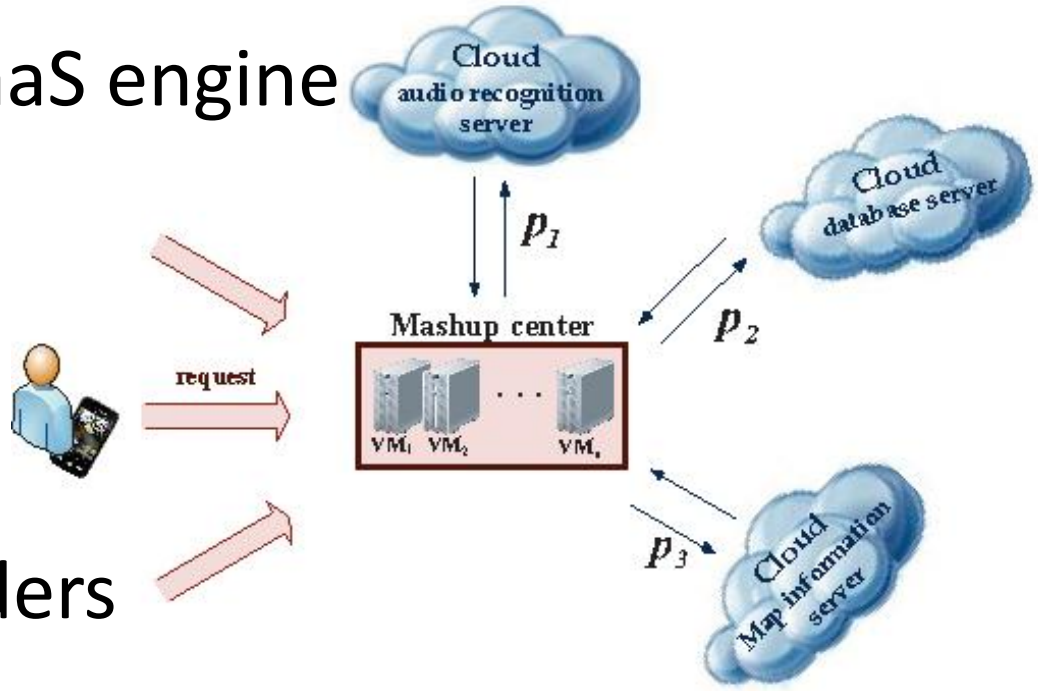
- Architecture Definitions:
  - Hybrid clouds change their composition and topology
  - Open and Extensible Architecture

Cloud Problems

- Single providers don’t have world coverage
- SaaS QoS expectations are different
- Outages
- Availability of Services
- Having all your eggs in the same basket

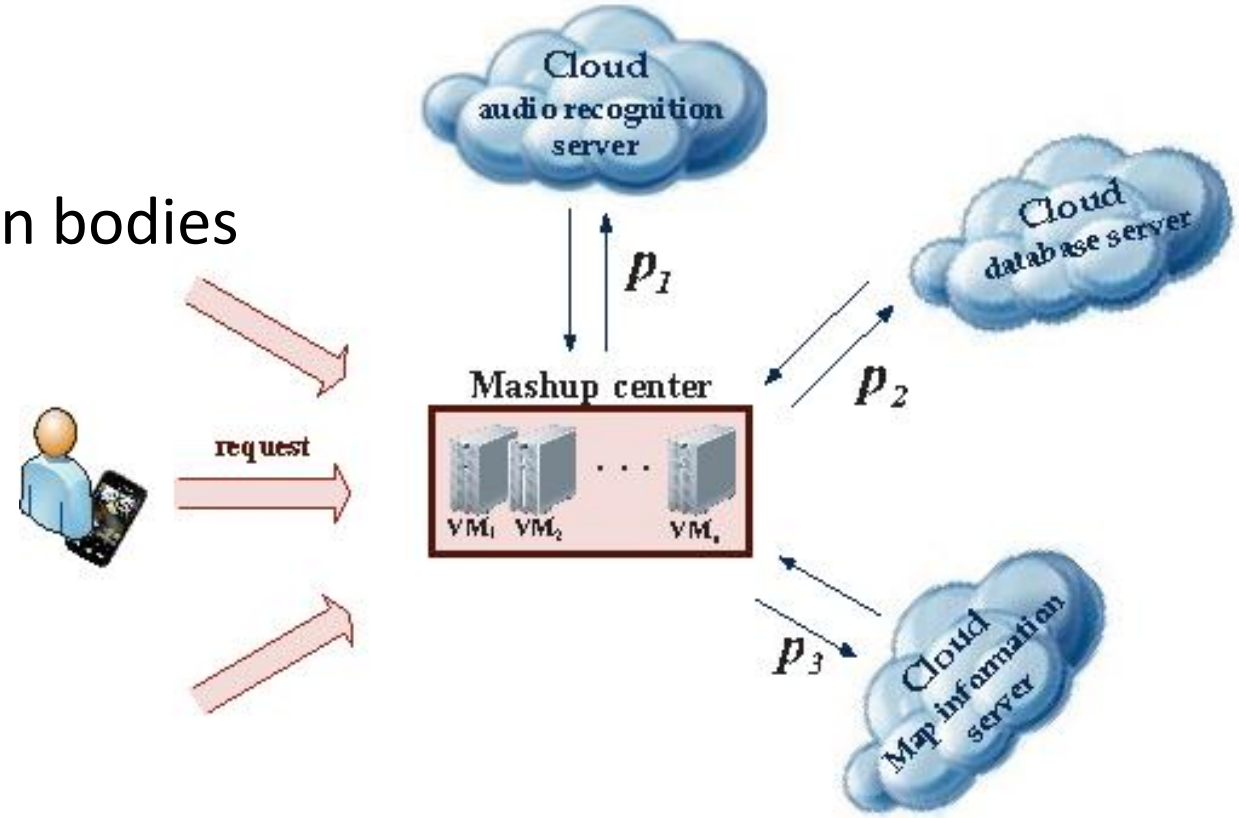
Solution: Cloud Mashups

- PaaS of a Federation of Clouds
- Compatibility of APIs and Programming Models
- Combine different APIs in a single PaaS engine
- Compatible VM for providing IaaS
- Interoperable Data structures
- Similar methods for swapping providers

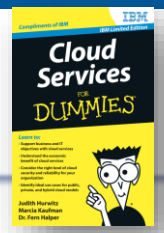


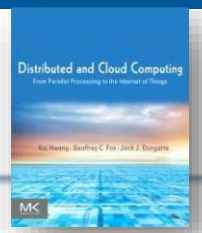
Solution: Cloud Mashups - Problems

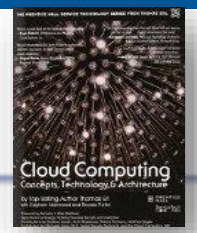
- Interoperability
  - Standardisation too slow to keep up with develop
  - Specifications diverge
  - Competition between standardisation bodies
- VM Image handling
- Data Management
  - Handling of huge amounts of data
  - Bandwidth to distribute the data

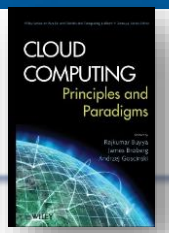


References









- Hwang, K., Fox, G., and Dongarra, J., “Distributed and Cloud Computing (From Parallel Processing to the Internet of Things)”, Elsevier, 2011
- Earl, T., Puttini, R., Mahmood, Z., “Cloud Computing: Concepts, Technology & Architecture”, Prentice-Hall, 2014
- Buyya, R., Broberg, J, Goscinski, A., “Cloud Computing Principles and Paradigms”, Wiley & Sons, 2011
- Herbst, N., Kounev, S., and Reussner, R., “Elasticity in Cloud Computing: What It Is, and What It Is Not”, in Proceedings of the 10th International Conference on Autonomic Computing (ICAC 2013), San Jose, June 24–28
- Smith, J., Nair, R., “The Architecture of Virtual Machines”, 2005, IEEE
- Josyula, V., Orr, M., Page, G., “Cloud Computing: Automating the Virtualized Data Center”, Cisco Press, 2012
- Ibrahim, K., Hofmeyr, S., Iancu, C., Roman, E., “Optimized Pre-Copy Live Migration for Memory Intensive Applications”, Proceedings of 2011 International Conference for High Performance Computing, Networking, Storage and Analysis, November 12-18, 2011, Seattle, Washington doi:10.1145/2063384.2063437
- Hurwitz, J., Kaufman, M., Halper, F., “Cloud Services for Dummies, IBM Limited Edition”, Wiley & Sons, 2012
- Paraïso, F., “Multi-Cloud PaaS”, Université Lille1
- Oracle Cloud Computing Strategy, http://www.oracle.com/technetwork/topics/entarch/architectural-strategies-for-cloud--128191.pdf
- https://kb.iu.edu/d/aoru
- https://www.forcepoint.com/cyber-edu/firewall
- https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html
- https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/
- https://searchsecurity.techtarget.com/definition/firewall
- https://reciprocitylabs.com/resources/what-is-cybersecurity/
- https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
- https://www.geeksforgeeks.org/devops/rsa-vs-ed25519-which-key-pair-is-right-for-your-security-needs/