Introduction and Security Frameworks

Alessandro Pellegrini
a.pellegrini@ing.uniroma2.it

What is a “secure computing system”?

25-09-23

- *The most secure computer is one that is turned off, cemented into the foundation of a building with a Faraday cage and has thermite anti-tamper protection.*
  - There is no such thing as a secure computer.

Non possiamo mai parlare di PC "sicuri", non esistono. Mai fidarsi, bisogna essere "paranoici"

- The hardware and software stack is complex
- Could you trust all the layers?
  - An example: the “Thompson Compiler” (Reflections on Trusting Trust - Ken Thompson)
  - Rootkits, at all levels

Quando compilo, chi mi dice che non venga introdotto nulla a mia insaputa? Stesso discorso per librerie e dipendenze ad ogni livello, tutto si basa sul " fidarsi", che non è una cosa ottimale.

- Security is only about rising the bar...

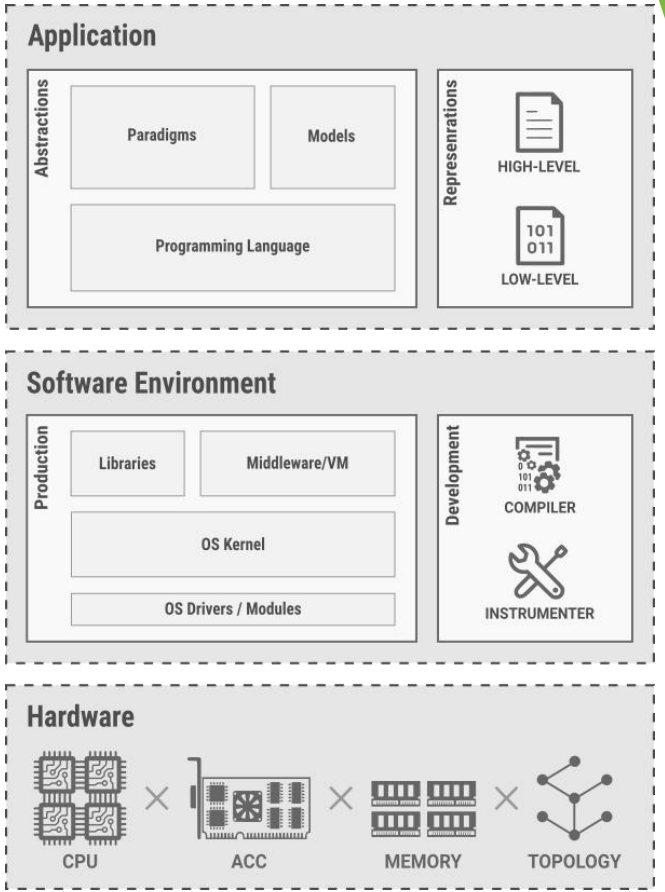
The IT Stak is Complex

Nulla è sicuro, neanche il S.O. Non esiste il full stack developer, perchè dovrebbe conoscere tutti i pericoli di tutti i livelli, cosa molto complessa.

- ICT development stacks are currently many
  - different problems to solve (*proficiency*)
  - different (distributed) hardware platforms can be used

- Tradeoffs:
  - Development time
  - Debugging time
  - Deployment cost
  - Maintenance
  - Vendor lock-in

- In the end, we want systems to just work!



The IT Stak is Complex

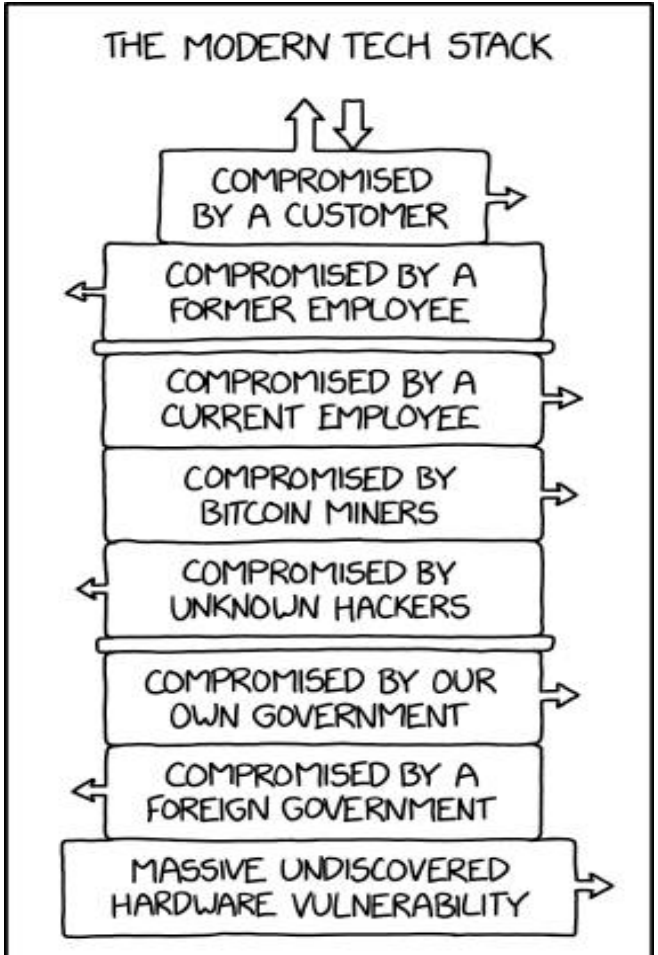
- ICT development stacks are currently many
  - different problems to solve (*proficiency*)
  - different (distributed) hardware platforms can be used

Devo essere paranoico quanto basta, altrimenti per paura non concluderò mai nulla. Dipende anche dal progetto.

- Tradeoffs:
  - Development time
  - Debugging time
  - Deployment cost
  - Maintenance
  - Vendor lock-in

L'user finale è una "scimmia", non devo sperare che sappia usare perfettamente il prodotto che fornisco.

- In the end, we want systems to just work!



Rationale behind security

1. Systems must be usable by legitimate users only
2. Access is granted on the basis of an authorization, and according to the rules that are established by some system administrator
    - As for point 1, an unusable system is useless
    - However, in several scenarios the attacker might only tailor system non-usability by legitimate users (DoS)

Un utente deve disporre di un "grant" basato su autorizzazione fornita da un admin ove necessario

Fundamental Security and Privacy Principles

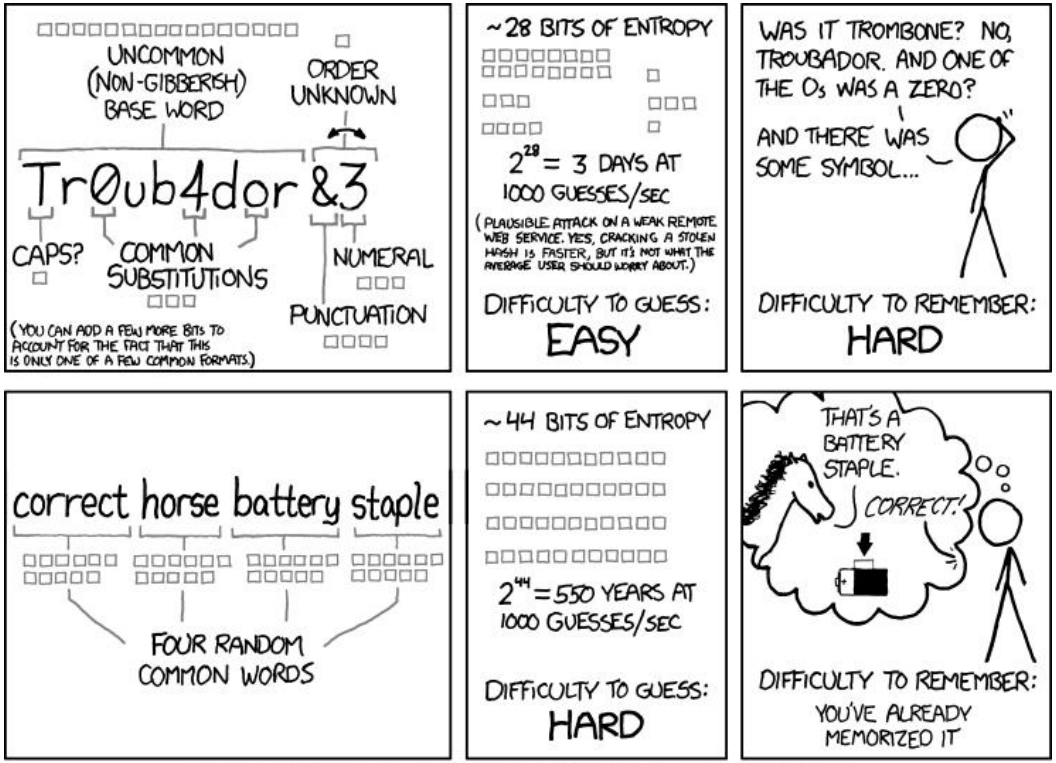
Baseline Security Principles

- Many IT experts and consulting companies stress a lot the following security aspects:
  - change your passwords and use strong ones
  - update your antivirus software
  - use a firewall

- While they are good security principles (and should be followed!), this is a naïve approach to security
- To increase the security of a system you must:
  - Look at the system from a system point of view
  - Look at the system from the perspective of humans
    - People involved in the system, to any extent
    - People from the outsite, who are interested in your business

Mai sottovalutare il sistema, anche scaricare un file sotto una vpn collegata a qualche sistema è pericoloso.

Strong Password Security



Questo meme ci dice che, contrariamente a ciò che si potrebbe pensare, è meglio una pw semplice ma lunga, piuttosto che complessa e corta. La complessità è solo per noi, ma chi poi va di brute force attack non vede differenze tra caratteri comuni e non.

Baseline Security Approaches

- Cryptography
- Authentication / Capabilities
- Security-enhanced operating systems

- Each approach targets specific security aspects
- They should be combined together to improve the overall security of the system

Se ho un DB in test, probabilmente userò un account root per testarlo in tutti i suoi aspetti. Ma ciò non è sicuro!

Principle of Least Privilege

- In a particular abstraction layer of a computing environment, entities must be able to access only the information and resources that are necessary for its legitimate purpose
  - Applies to processes, users, programs, virtual instances, ...

devo avere sempre le minori autorizzazioni possibili, per ridurre la superficie d'attacco.

- *Better system stability*: it is easier to test possible actions of the applications/users and interactions with other applications.
- *Better system security*: vulnerabilities in one application cannot be used to exploit the rest of the machine.
- *Ease of deployment*: the fewer privileges an application requires the easier it is to deploy within a larger environment.

Inoltre, se un utente ha privilegio A e B è diverso da avere privilegio A o B, dovrei fare più autorizzazioni a grana fine, ma questo rallenta lo sviluppo.

Need-to-know Principle

Se ho un privilegio x da usare in occasione y, dovrei poterlo usare solo in quel caso, non in altri casi.

- A user shall only have access to the information that their job function requires, regardless of their security clearance level or other approvals.
- The need-to-know principle is strictly bound to the real requirement for the user to fullfil its current goal.

- "Social engineering" problems:
  - it can be misused by persons who wish to refuse others access to information they hold in an attempt to increase their personal power;
  - it can prevent unwelcome review of people's work;
  - it can be used to prevent embarrassment resulting from actions or thoughts.

Cryptography

- Cryptography is a technique to obfuscate information so as to guarantee data confidentiality

  - **E** = encryption function & **D** = decryption function
  - **K1** = encryption key & **K2** = decryption key
  - **d** = clear data & **c** = encrypted data
  - $E_{K1}[d] \Longrightarrow c$ & $D_{K2}[c] \Longrightarrow d$

- Cryptography is *probabilistically secure*
  - You can always try all keys to break encryption
  - That's regarded as *computationally unfeasible*, typically

Offuscamento dei dati, ruolo importante è dato dalle chiave (gli algoritmi sono "noti", il segreto non è in loro), senza chiavi il lavoro sarebbe molto più lungo. Abbiamo crittografia simmetrica ed asimmetrica.

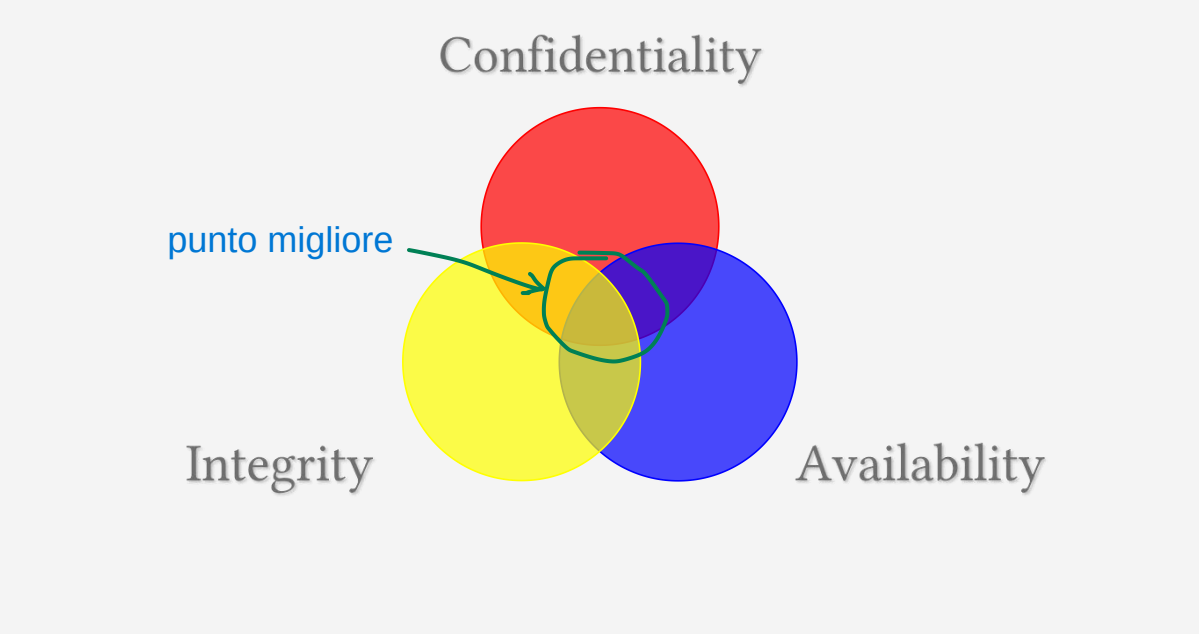
Cryptography

- There are two main approaches to cryptography

- *Symmetric Cryptography* (K1=K2)
  - Each couple (or group) of entities exchangin/accessing data share a pre-known key

- As*ymmetric Cryptography* (K1≠K2)
  - Each entity maintains a private key which is never shared
  - The corresponding public key is shared and know to the world
  - Enables also digital signing

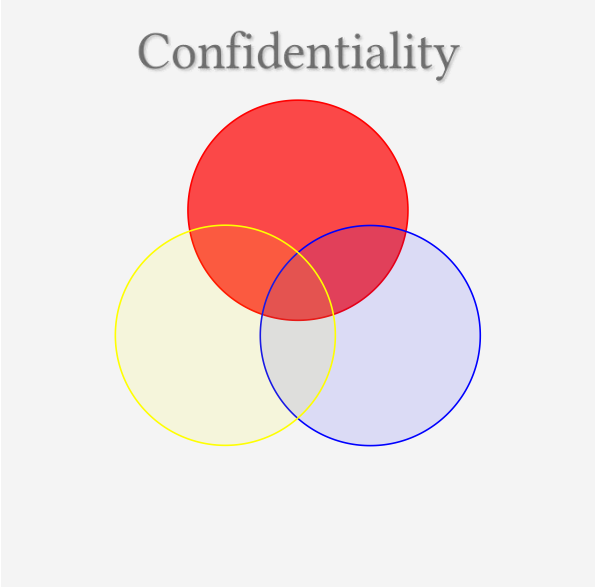
CIA: the building blocks



Confidentiality

Simile al primo principio, ma visto da una prospettiva diversa.

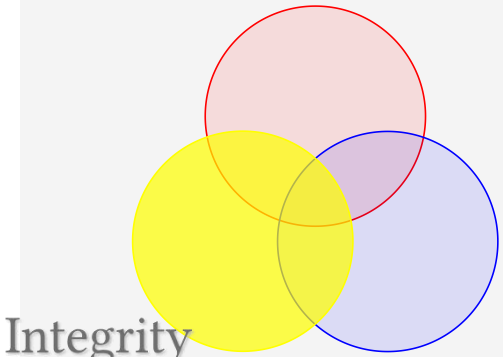
- You are not allowed to access data if you are not allowed
- Accomplished through encryption:
  - https://
  - s/mime
  - pgp
  - ssh and ipsec



Integrity

- You are unable to alter data if you are not allowed to
- Integrity is increased by proper data and system management

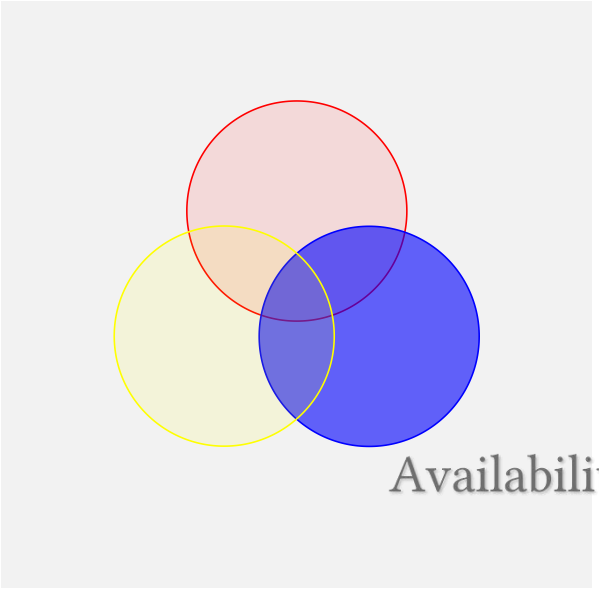
Possiamo vederlo come un insieme dei due principi. Anche fisicamente abbiamo necessità di nascondere un backup per preservare i dati, che non devono essere alterati da chi non ha tale ruolo.



Availability

- Ensures that the system works promptly and the service is not denied to authorized users
- In critical infrastructures, Availability may become by far the most important security objective!

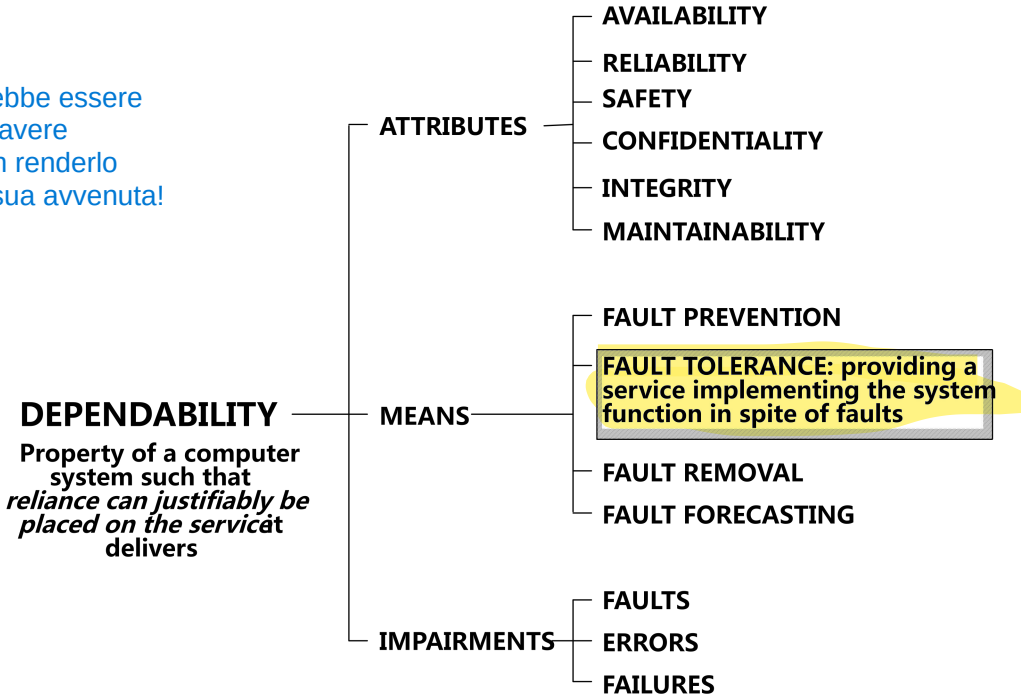
Sembra slegato ai primi due, tuttavia molti attacchi hanno come obiettivo ridurre la disponibilità di un servizio. Spesso si parla direttamente di dependability.



Even Better: Dependability

- **Dependability**: "*the trustworthiness of a computing system which allows reliance to be justifiably placed on the service it delivers*"

Il sistema dovrebbe essere sicuro prima di avere il problema, non renderlo sicuro dopo la sua avvenuta!



Other Security Objectives

- Authenticity certificare sorgente con cui abbiamo interazione
  - Aauthentication: ability to verify that a user is the one they claim to be
  - source authenticity (non repudiability): ability to verify that a message comes from the actual trusted origin
    - More precise than just data integrity
- Access control (Authorization) utente ha il permesso di fare una certa operazione?
  - ability to verify that a user has the permission to perform some activity
- Accountability tracciamento delle abilità. E' la più ignorata, poichè costosa in termini manageriali.
  - ability to trace actions of an entity, including the recording of such actions in a log-file for later-on forensic analysis

Security Frameworks

Why Security Frameworks?

- The complexity of computer systems is increasing
- Threats are always diverse
- The baseline security principles that we have discussed can cope with many threats, but are very general

- There is a need to standardise security practices

- A security framework provides a structured approach to information security
- They enable organizations to *identify*, *manage*, and *mitigate* risks in a *consistent* and *repeatable* manner

FIPS 200

E' un set minimale di "consigli". Sono dei principi, non c'è nulla di specifico.
Dettagli in più sono a pagamento.

- Minimum security requirements for federal information and information systems
- It defines several fundamental objectives for a “secure” system

- **Access control**: Limit information system access to authorised users, processes acting on behalf of authorised users or devices (including other information systems), and the types of transactions and functions authorised users are permitted to exercise.

Descrizione di cosa fanno i vari tipi di utenti.

FIPS 200

- **Awareness and training**: (i) Ensure that managers and users of organisational information systems are made aware of the security risks associated with their activities and of the applicable laws, regulations, and policies related to the security of organisational information systems; and (ii) ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities. Istruire/allenare gli utenti, evitando che compiano azioni non previste/non sicure. (esempio base: password banali, password stampare in chiaro, download di cose strane...)

- **Audit and accountability**: (i) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorised, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions. Monitoraggio delle attività

FIPS 200

- **Certification, accreditation, and security assessments**:
  - Periodically assess the security controls in organisational information systems to determine if the controls are effective in their application.
  - Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organisational information systems
  - Authorise the operation of organisational information systems and any associated information system connections
  - Monitoring information system security controls on an ongoing basis to ensure the continued effectiveness of the controls

La sicurezza è in continua evoluzione, non finisce mai, bisogna sempre aggiornarsi!

FIPS 200

- **Configuration management**: (i) Establish and maintain baseline configurations and inventories of organisational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organisational information systems.

  Se il sistema cresce, è facile perdere il controllo della gestione, bisogna quindi anche aggiornare le informazioni possedute (pc nuovi, non in uso devono essere scollegati, etc...)

- **Contingency planning**: Establish, maintain, and implement plans for emergency response, backup operations, and postdisaster recovery for organisational information systems to ensure the availability of critical information resources and continuity of operations in emergencies.

  E' impossibile che tutto vada bene, prima o poi subiremo un attacco, bisogna essere pronti alle varie evenienze.
  Ad esempio, so che un pc/componente potrà rompersi, allora è importante avere un backup!

FIPS 200

- **Identification and authentication**: Identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices as a prerequisite to allowing access to organisational information systems.
  chi sono gli utenti? cosa fanno gli utenti?

- **Incident response**: (i) Establish an operational incident handling capability for organisational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organisational officials and/or authorities.
  se avviene un incidente, devo carpire più informazioni possibili: quali file ha toccato? quali componenti ha toccato?

FIPS 200

- **Maintenance**: (i) Perform periodic and timely maintenance on organisational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Periodicamente, sarebbe buona norma vedere se sono presenti errori da fixare, non devo "aspettare il disastro".
A volte riesco infatti a prevenire, ad esempio l'usura di una componente.

CIS Security Controls

Catturano gli aspetti appena visti, rendendoli però più applicabili. Abbiamo diversi livelli di sicurezza.
Noi li esamineremo a diversi livelli dello stack, partendo dall'hardware a salire.

- 20 practical controls
  - https://www.sans.org/critical-security-controls
  - each control further detailed in sub-controls
- Easy to apply also in small enterprises
- Prioritized: the first 5 controls (*foundational Cyber Hygiene*) are basic (account for 85% threats)
  - ***CSC 1:*** Inventory of Authorized and Unauthorized Devices
  - ***CSC 2:*** Inventory of Authorized and Unauthorized Software
  - ***CSC 3:*** Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
  - ***CSC 4:*** Continuous Vulnerability Assessment and Remediation
  - ***CSC 5:*** Controlled Use of Administrative Privileges

CIS Critical Security Controls 1-2

- Know and continuously track your HW/SW assets!
- **CSC 1: Inventory of Authorized and Unauthorized Devices**
  - Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access
- **CSC 2: Inventory of Authorized and Unauthorized Software**
  - Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution

CIS CSC: very practical sub-controls!

Critical Security Control #1: Inventory of Authorized and Unauthorized Devices	
System 1.1	Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.
System 1.2	If the organization is dynamically assigning addresses using DHCP, then deploy dynamic host configuration protocol (DHCP) server logging, and use this information to improve the asset inventory and help detect unknown systems.
System 1.3	Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.
System 1.4	Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.
System 1.5	Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems.
System 1.6	Use client certificates to validate and authenticate systems prior to connecting to the private network.

CIS Critical Security Controls 3-4

- Continuously check (configs) and patch (vulnerabilities)

- **CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**
  - Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings
- **CSC 4: Continuous Vulnerability Assessment and Remediation**
  - Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers

Remaining CIS CSC

- ***CSC 5:*** Controlled Use of Administrative Privileges
- ***CSC 6:*** Maintenance, Monitoring, and Analysis of Audit Logs
- ***CSC 7:*** Email and Web Browser Protections
- ***CSC 8:*** Malware Defenses
- ***CSC 9:*** Limitation and Control of Network Ports, Protocols, and Services
- ***CSC 10:*** Data Recovery Capability
- ***CSC 11:*** Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- ***CSC 12:*** Boundary Defense
- ***CSC 13:*** Data Protection
- ***CSC 14:*** Controlled Access Based on the Need to Know
- ***CSC 15:*** Wireless Access Control
- ***CSC 16:*** Account Monitoring and Control
- ***CSC 17:*** Security Skills Assessment and Appropriate Training to Fill Gaps
- ***CSC 18:*** Application Software Security
- ***CSC 19:*** Incident Response and Management
- ***CSC 20:*** Penetration Tests and Red Team Exercises

ISO/IEC 27000

- The ISO/IEC 27000 series “Information Security Management Systems (ISMS) Family of Standards” is an information security standard drawn up by ISO
- Also known in Italy as the SGSI family of standards (Information Security Management Systems)
- It groups together a set of international standards that aim to protect the information that is maintained and processed by an organisation.

- Companies can obtain an official certification of their compliance to the standard

ISO/IEC 27000

#	Standard	Published	Title	Notes
1	ISO/IEC 27000	2018	Information security management systems — Overview and vocabulary	Overview/introduction to the ISO27k standards as a whole plus a glossary of terms; FREE!
2	ISO/IEC 27001	2013	Information security management systems — Requirements	Formally specifies an ISMS against which thousands of organizations have been certified compliant
3	ISO/IEC 27002	2013	Code of practice for information security controls	A reasonably comprehensive suite of information security control objectives and generally-accepted good practice security controls
4	ISO/IEC 27003	2017	Information security management system implementation guidance	Sound advice on implementing ISO27k, expanding section-by-section on the main body of ISO/IEC 27001
5	ISO/IEC 27004	2016	Information security management — Measurement	Much improved second version, with useful advice on security metrics
6	ISO/IEC 27005	2018	Information security risk management	Discusses information risk management principles in general terms without specifying or mandating particular methods. Major revision in progress

ISO/IEC 27000

#	Standard	Published	Title	Notes
7	ISO/IEC 27006	2015	Requirements for bodies providing audit and certification of information security management systems	Formal guidance for the certification bodies, with several grammatical errors – needs revision
8	ISO/IEC 27007	2017	Guidelines for information security management systems auditing	Auditing the management system elements of the ISMS
9	ISO/IEC TR 27008	2011	Guidelines for auditors on information security controls	Auditing the information security elements of the ISMS
10	ISO/IEC 27009	2016	Sector-specific application of ISO/IEC 27001 – requirements	Guidance for those developing new ISO27k standards (i.e. ISO/IEC JTC1/SC27 – an internal committee standing document really)
11	ISO/IEC 27010	2015	Information security management for inter-sector and inter-organisational communications	Sharing information on information security between industry sectors and/or nations, particularly those affecting "critical infrastructure"
12	ISO/IEC 27011	2016	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	Information security controls for the telecoms industry; also called "ITU-T Recommendation x.1051"
13	ISO/IEC 27013	2015	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	Combining ISO27k/ISMS with IT Service Management/ITIL
14	ISO/IEC 27014	2013	Governance of information security	Governance in the context of information security; will also be called "ITU-T Recommendation X.1054"
16	ISO/IEC TR 27016	2014	Information security management – Organizational economics	Economic theory applied to information security

ISO/IEC 27000

#	Standard	Published	Title	Notes
17	ISO/IEC 27017	2015	Code of practice for information security controls for cloud computing services based on ISO/IEC 27002	Information security controls for cloud computing
18	ISO/IEC 27018	2014	Code of practice for controls to protect personally identifiable information processed in public cloud computing services	Privacy controls for cloud computing
19	ISO/IEC TR 27019	2017	Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry	Information security for ICS/SCADA/embedded systems (not just used in the energy industry!), excluding the nuclear industry
20	ISO/IEC 27021	2017	Competence requirements for information security management professionals	Guidance on the skills and knowledge necessary to work in this field
21	ISO/IEC 27023	2015	Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002	Belated advice for those updating their ISMSs from the 2005 to 2013 versions
22	ISO/IEC 27030	DRAFT	Guidelines for security and privacy in Internet of Things (IoT)	A standard about the information risk, security and privacy aspects of IoT
23	ISO/IEC 27031	2011	Guidelines for information and communications technology readiness for business continuity	Continuity (i.e. resilience, incident management and disaster recovery) for ICT, supporting general business continuity
24	ISO/IEC 27032	2012	Guidelines for cybersecurity	Ignore the vague title: this standard actually concerns Internet security
25	ISO/IEC 27033	-1 2015	Network security overview and concepts	Various aspects of network security, updating and replacing ISO/IEC 18028